

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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a purple header bar with the title "Microsoft 365 admin center". Below it, a navigation sidebar on the left lists "Users", "Active users" (which is selected and highlighted in blue), "Contacts", "Guest users", and "Deleted users". The main content area features a large banner with the text "Setup Microsoft 365 E5 (no Teams)" and a callout pointing to the "Add users" button. Below the banner, there are three cards: "Add domain", "Add users", and "Connect domain". A blue button at the bottom left says "Go to guided setup". In the bottom right corner of the main content area, there are two small icons: a speech bubble and a gear. At the very bottom of the screen, a URL bar shows the address "https://admin.microsoft.com/#/users".

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The title bar displays "Amit - 101572711" and the URL "admin.microsoft.com/#/users". The main header says "Microsoft 365 admin center". Below it, the breadcrumb navigation shows "Home > Active users". On the right, there's a "Enable Dark mode" button. The main content area is titled "Active users". It features a toolbar with buttons for "Add a user", "User templates", "Add multiple users" (which is highlighted in blue), and a search bar. A filter dropdown is set to "Commonly used" with options for "Licenses", "Sign-in status", "Domain", and "Location". The main table lists 13 active users:

	Display name ↑	Username	Licenses
<input type="checkbox"/>	101572711	101572711@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	Alice Walker	alice.walker@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	Amit Ratnaparkhi	ARGBC2025@ARGBC2025.onmicrosoft.com	Microsoft Power Apps for Automate Free, Microsoft
<input type="checkbox"/>	Bob Carter	bob.carter@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	dynamicUser1	dynamicUser1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	Exchange-Admin	Exchange-Admin@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	GBTESTSHARED1	GBTESTSHARED1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	helpdesk	helpdesk@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	sally	sally@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	task2 user1	user1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	task2 user2	user2@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
<input type="checkbox"/>	Toronto	Toronto@ARGBC2025.onmicrosoft.com	Microsoft 365 E5

I then add multiple users

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The title bar says "Amit - 101572711 Microsoft 365 admin". The left sidebar has a "AR GBC 2025" profile icon and navigation links: Home, Active users, Add multiple users, Basics (which is selected), Licenses, and Finish. The main content area is titled "Add list of users" and says "Enter up to 249 users. All users are given temporary passwords." It features a table with columns: First name, Last name, Username, and Domain. There are five rows of input fields, each with "First name", "Last name", "Username" (prefilled with "ARGBC2025.onmi...") and "Domain" (prefilled with "ARGBC2025.onmi..."). Below the table is a checkbox for "I'd like to upload a CSV with user information". At the bottom, there's a link "Learn how to add multiple users" and a small preview window showing the "Active users" screen. Buttons at the bottom are "Next" and "Cancel".

I choose to upload a CSV

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface for adding multiple users. The left sidebar has icons for Home, Users, Licenses, and Finish. The main area shows the 'Active users > Add multiple users' screen. A progress bar on the left indicates the 'Basics' step is selected. Below it are 'Licenses' and 'Finish' steps. The main form has five rows for entering user information: First name, Last name, Username, and Domain (set to @ARGBC2025.onmi...). A checkbox labeled 'I'd like to upload a CSV with user information' is checked. Below it is a note: 'Download one of the files below. Open the file in Excel or a similar app, add user info, save, and upload.' with a link to 'Download a blank CSV file with the required headers'. There is also a link to 'Download a CSV file that includes example user info'. A field for 'Upload CSV file with your user information *' has a 'Browse' button. At the bottom, there are 'Next' and 'Cancel' buttons.

I download a blank CSV template

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the URL <http://www.namecheap.com/domains/domaincontrolpanel/techsolutionsinc.store>. The page is titled 'Domains → Details' for the domain 'techsolutionsinc.store'. The left sidebar has a dark theme with light-colored icons and text, listing 'Dashboard', 'Expiring / Expired', 'Domain List' (which is selected), 'Hosting List', 'Private Email', 'SSL Certificates', 'Apps', 'My Offers' (with a 'NEW' badge), and 'Profile'. The main content area shows the domain 'techsolutionsinc.store' with a green header bar. Below it, there are sections for 'STATUS & VALIDITY' (Active, April 12, 2025 - April 12, 2026, Auto-renew off, Add Years button) and 'Withheld for Privacy' (Protection off, Auto-renew off, Add Years button). A 'PremiumDNS' section offers protection for \$19.99 per year, with a 'BUY NOW' button. At the bottom, there are sections for 'NAMESERVENS' (set to 'Namecheap BasicDNS') and 'REDIRECT DOMAIN' (set to 'techsolutionsinc.store' with the URL 'http://www.techsolutionsinc.store/'). A small trash can icon is visible next to the redirect URL.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a purple header with the user's name and ID (Amit - 101572711). The main navigation bar includes links for Mail, Domain, and other services. The main content area is titled "Finish setting up Microsoft 365 E5 (no Teams)". It features a callout diagram with three overlapping cards: "Add domain" (blue), "Add users" (white), and "Connect domain" (light blue). Below the diagram is a button labeled "Go to guided setup". To the right, there's a "User management" section with a sub-section titled "User management" and a note: "Add, edit, and remove user accounts, and reset passwords." A small sidebar on the right contains icons for Help, Feedback, and Chat.

I connect the domain to MS365

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The title bar displays "Amit - 101572711" and the URL "https://admin.microsoft.com/#/Domains/Wizard". The left sidebar has a "Domains" icon. The main content area is titled "Add domain" and shows a flowchart with four steps: "Add domain" (selected), "Domain name" (highlighted with a blue dot), "Connect domain", and "Finish". To the right, the "Domain name" step is expanded, showing the input field "techsolutionsinc.store". Below it is a video thumbnail titled "Learn how to add a domain" with a play button. A tooltip says "Play this video to learn how to add a domain". At the bottom, there are buttons for "Use this domain" and "Close".

I add the domain

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The top navigation bar includes tabs for 'Mail', 'Domain', and 'Identity'. The main title is 'Amit - 101572711'. The left sidebar has a 'Domains' icon. The main content area is titled 'Domains > Add domain'. A vertical flowchart on the left indicates the steps: 'Add domain' (selected), 'Domain name', 'Domain verification' (selected), 'Connect domain', and 'Finish'. To the right, the main content area says 'Verify you own your domain'. It explains that before setting up the domain, the user needs to verify ownership. Three options are listed: 1) 'Add a TXT record to the domain's DNS records' (selected), which is recommended for creating new DNS records. 2) 'If you can't add a TXT record, add an MX record to the domain's DNS records' (not selected), which is recommended if TXT records are unsupported. 3) 'Add a text file to the domain's website' (not selected), which is recommended for existing websites. Below this, there is a link to 'Learn how to add a TXT record' and a video thumbnail titled 'Verify your domain with'. At the bottom are 'Back', 'Continue' (highlighted in blue), and 'Close' buttons.

I add the TXT

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Namecheap Advanced DNS interface. The left sidebar menu includes Dashboard, Expiring / Expired, Domain List (selected), Hosting List, Private Email, SSL Certificates, Apps, My Offers (NEW), and Profile. The main content area displays two DNS records:

- URL Redirect Record**:
 - Type: URL Redirect Record
 - Host: @
 - Destination URL: <http://www.techsolutionsinc.store/>
 - Status: Unmasked
- TXT Record**:
 - Type: TXT Record
 - Host: @
 - Value: MS=ms21371835
 - TTL: Automatic

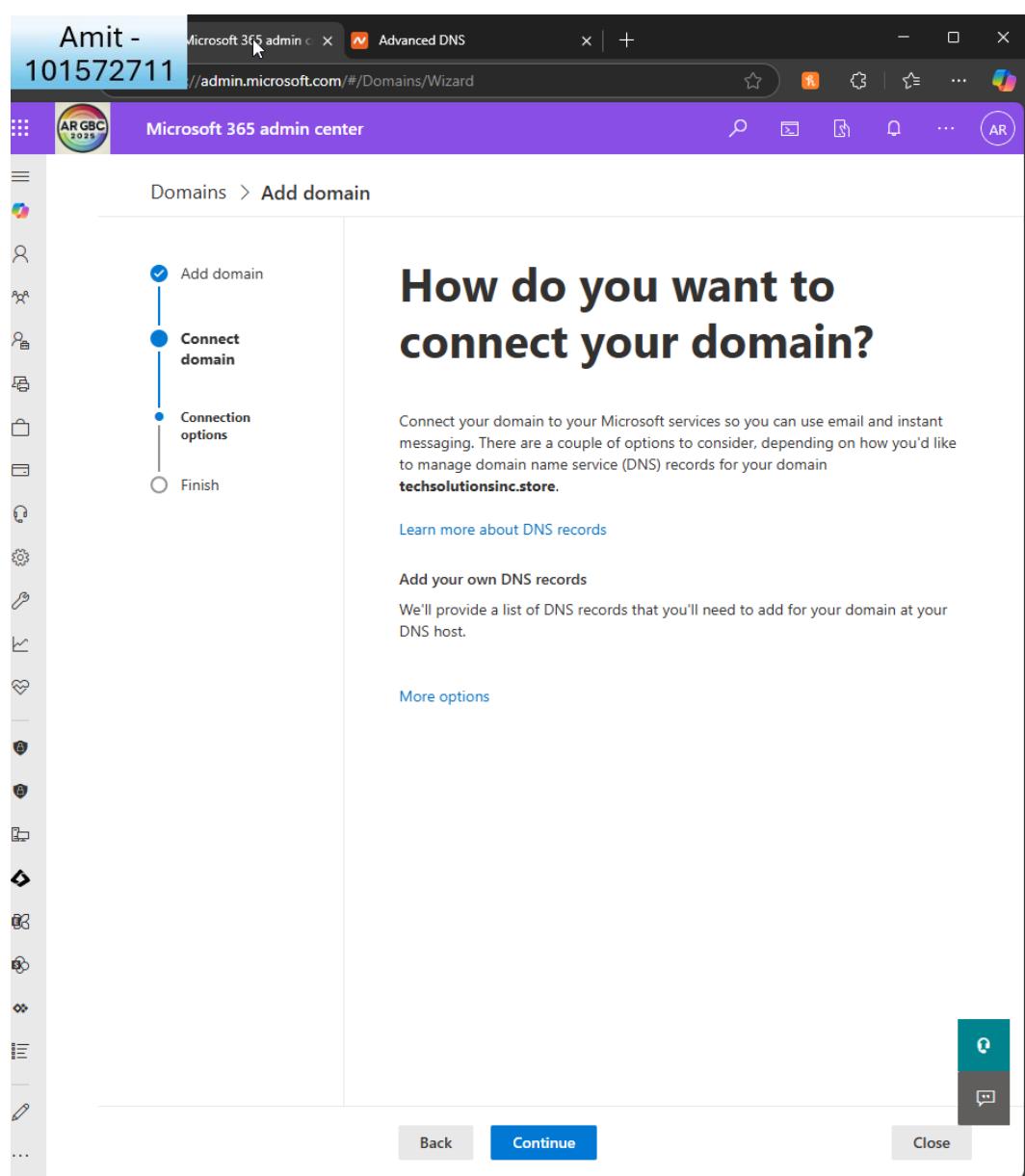
At the bottom, there are buttons for DNSSEC, Status (disabled), Mail Settings, and Email Forwarding.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



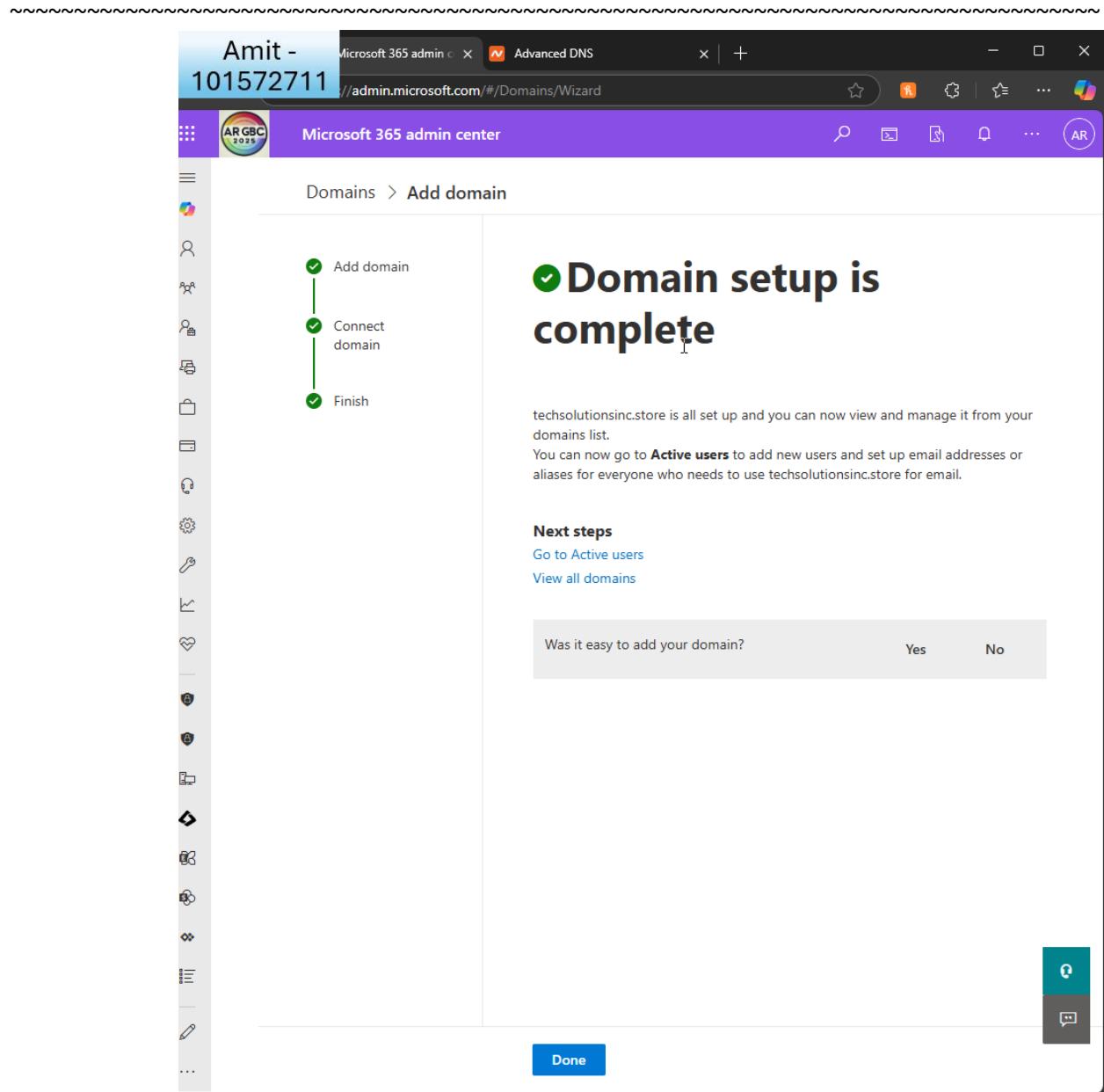
I go back to admin centre to connect the domain

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I also made sure the MX and TXT records are correct

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center Domains page. At the top, there's a navigation bar with icons for users, groups, roles, and more. Below it, the main title is "Domains". On the left, there's a sidebar with various administrative icons. The main content area displays a table of domains:

Domain name ↑	Status
techsolutionsinc.store (Default)	Healthy
ARGBC2025.onmicrosoft.com	Healthy

At the bottom right of the table, there are buttons for "Choose columns" and a search bar labeled "Search domains".

I can see my domain now and it's default

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Excel spreadsheet titled "techsolutions_users". The data consists of 11 columns: Username, First name, Last name, Display name, Job title, Department, Office num, and Office pho. The data is as follows:

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

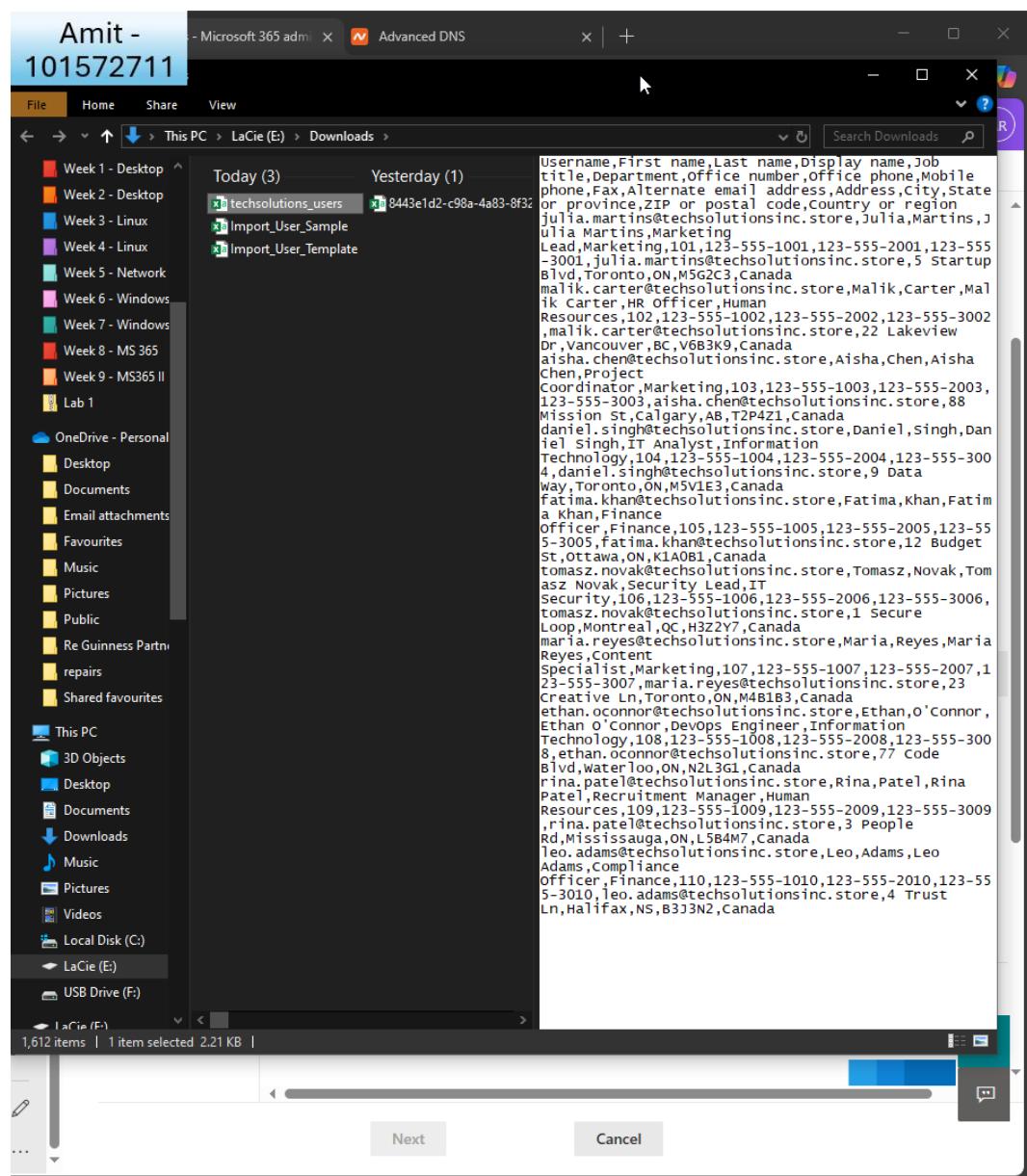
I used chatGPT to fill the CSV file with information

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface for adding multiple users. The top navigation bar includes 'Advanced DNS' and the URL [//admin.microsoft.com/#/addmultipleusers](https://admin.microsoft.com/#/addmultipleusers). The left sidebar has various icons for managing users, groups, and devices. The main content area is titled 'Active users > Add multiple users'. A vertical progress bar on the left indicates the 'Basics' step is selected, followed by 'Licenses' and 'Finish'. Below the progress bar are six sets of input fields for 'First name', 'Last name', 'Username', and '@techsolutionsinc.st...'. A checked checkbox below the fields says 'I'd like to upload a CSV with user information'. A tooltip provides instructions: 'Download one of the files below. Open the file in Excel or a similar app, add user info, save, and upload.' Below the CSV section are links to download blank or example CSV files. A 'Browse' button is available to upload a CSV file. At the bottom are 'Next' and 'Cancel' buttons.

I upload the file

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

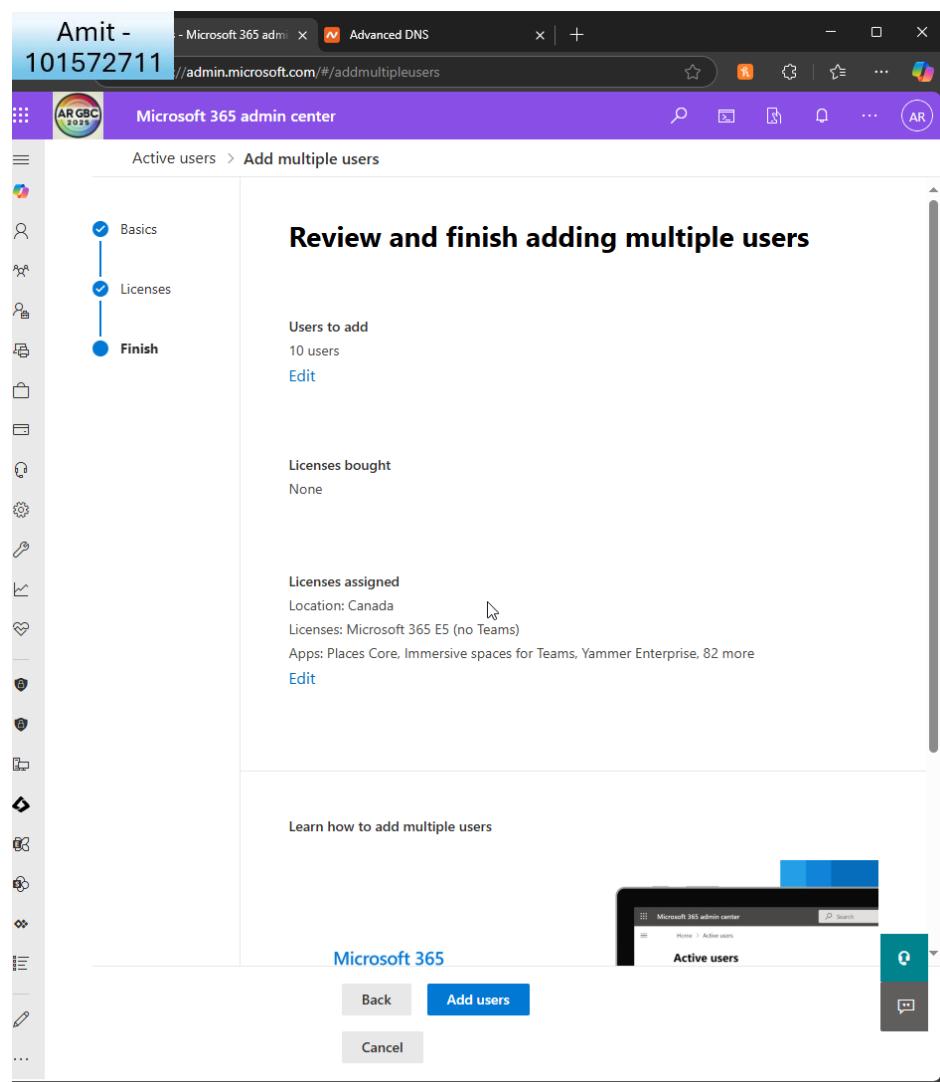
Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, the URL is `https://admin.microsoft.com/#/addmultipleusers`. On the left, there's a sidebar with various icons. A vertical navigation bar on the right indicates the steps: Basics (checked), Licenses (checked), and Finish (unchecked). The main content area is titled "Licenses" and contains the following text: "Select the location and product licenses for the **10 users** you're adding." Below this, a "Location" dropdown is set to "Canada". Under the "Licenses" section, the "Assign licenses" radio button is selected. It lists four options: "Microsoft 365 E3 (no Teams)" (unchecked), "Microsoft 365 E5 (no Teams)" (checked), "Microsoft Power Apps for Developer" (unchecked), and "Microsoft Power Automate Free" (unchecked). There's also an option "Don't assign any licenses (not recommended)". At the bottom, there are "Back", "Next", and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

I review and finish adding multiple users

The screenshot shows the Microsoft 365 Admin Center interface. The title bar indicates the user is 'Amit - 101572711'. The main title is 'Active users > Add multiple users'. On the left, there's a vertical navigation menu with various icons. In the center, a summary message says 'You added 10 users' with a checkmark icon. Below it, a note states: 'These users will appear in your list of **Active users** where you can view and manage their settings. All users have been given temporary passwords and they can now log in to their accounts.' At the bottom, there are 'Print' and 'Download user details' buttons, followed by a table of user information:

Display name	Username
Julia Martins	julia.martins@techsolutionsinc.store
Malik Carter	malik.carter@techsolutionsinc.store
Aisha Chen	aisha.chen@techsolutionsinc.store
Daniel Singh	daniel.singh@techsolutionsinc.store
Fatima Khan	fatima.khan@techsolutionsinc.store
Tomasz Novak	tomasz.novak@techsolutionsinc.store
Maria Reyes	maria.reyes@techsolutionsinc.store
Ethan O'Connor	ethan.oconnor@techsolutionsinc.store
Rina Patel	rina.patel@techsolutionsinc.store
Leo Adams	leo.adams@techsolutionsinc.store

A blue 'Close' button is at the bottom right of the table area.

2. Configure User Profiles:

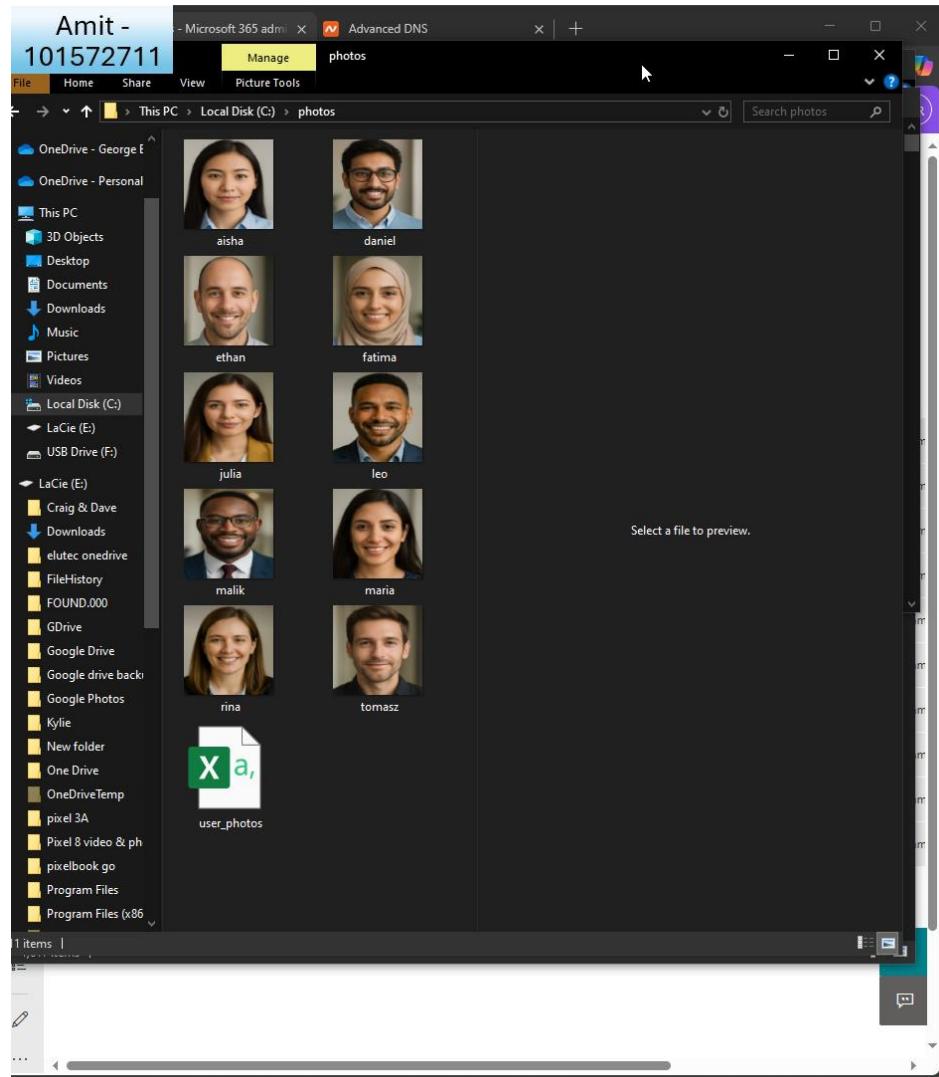
Microsoft 365 Identity and Services – Enterprise Administration

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft 365 Admin PowerShell window titled "Amit - 101572711". The window displays a PowerShell script for uploading user photos from a CSV file. The script uses the Microsoft.Graph module to connect to the Microsoft Graph API and update user profiles. The code includes error handling for failed uploads.

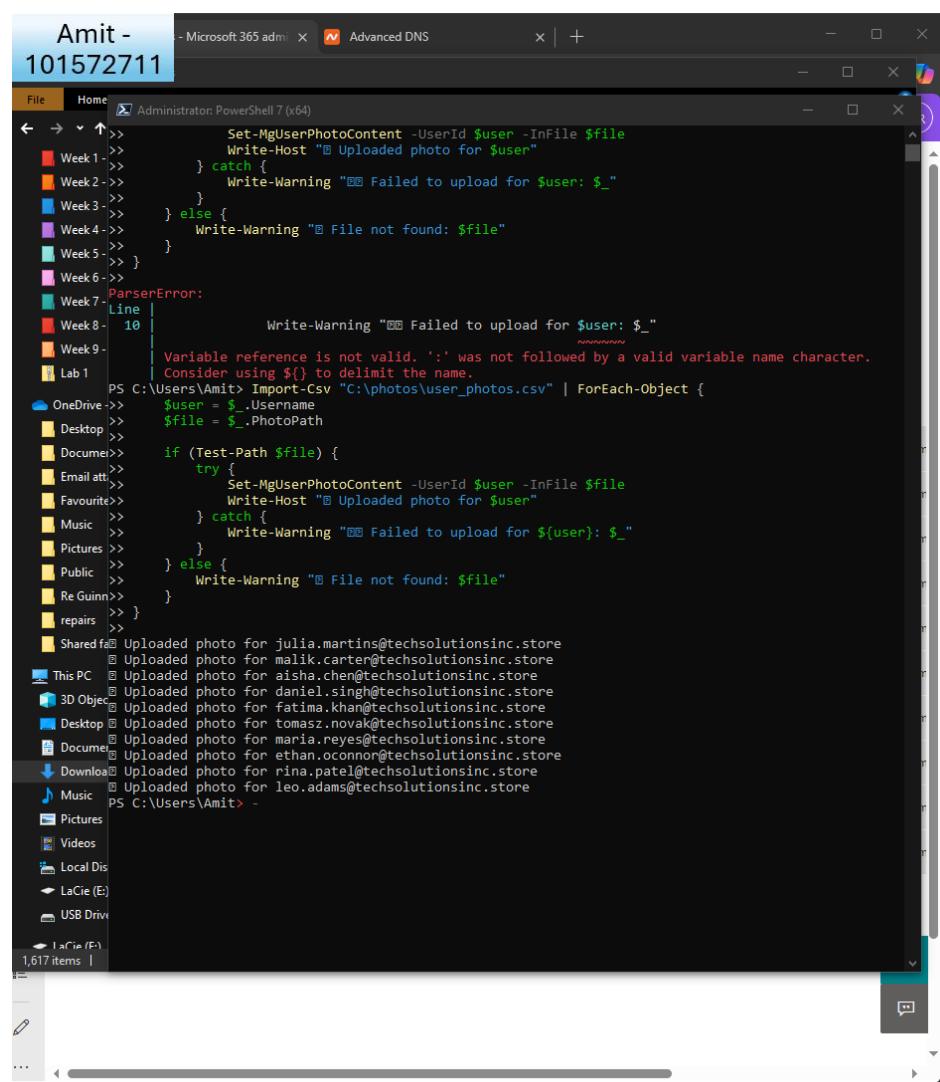
```
PS C:\Users\Amit> Install-Module Microsoft.Graph -Scope CurrentUser
PS C:\Users\Amit> Connect-MgGraph -Scopes "User.ReadWrite.All"
Welcome to Microsoft Graph!
PS C:\Users\Amit> Import-Csv "C:\photos\user_photos.csv" | ForEach-Object {
    $user = $_.Username
    $file = $_.PhotoPath
    if (Test-Path $file) {
        try {
            Set-MgUserPhotoContent -UserId $user -InFile $file
            Write-Host "Uploaded photo for $user"
        } catch {
            Write-Warning "Failed to upload for $user: $_"
        }
    } else {
        Write-Warning "File not found: $file"
    }
}
1,617 items
```

I use this script to set the photo in the profile

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



The screenshot shows a Microsoft 365 Admin Center interface with a PowerShell window titled "Amit - 101572711". The PowerShell session is titled "Administrator: PowerShell 7 (x64)". The command being run is:

```
Set-MgUserPhotoContent -UserId $user -InFile $file
    Write-Host "Uploaded photo for $user"
} catch {
    Write-Warning "Failed to upload for $user: $_"
} else {
    Write-Warning "File not found: $file"
}
}

Week 6 >>
ParserError:
Week 7 >> Line | 10 |     Write-Warning "Failed to upload for $user: $_"
Week 9 >>     Variable reference is not valid. ':' was not followed by a valid variable name character.
Lab 1 | Consider using ${} to delimit the name.

PS C:\Users\Amit> Import-Csv "C:\photos\user_photos.csv" | ForEach-Object {
    $user = $_.Username
    $file = $_.PhotoPath
    if (Test-Path $file) {
        try {
            Set-MgUserPhotoContent -UserId $user -InFile $file
            Write-Host "Uploaded photo for $user"
        } catch {
            Write-Warning "Failed to upload for $user: $_"
        }
    } else {
        Write-Warning "File not found: $file"
    }
}
Re Gunn>>
repairs >>
Shared folder Uploaded photo for julia.martins@techsolutionsinc.store
 Uploaded photo for malik.carter@techsolutionsinc.store
This PC  Uploaded photo for aisha.cheng@techsolutionsinc.store
 3D Objects  Uploaded photo for daniel.singh@techsolutionsinc.store
Desktop  Uploaded photo for fatima.khan@techsolutionsinc.store
Documents  Uploaded photo for maria.reyes@techsolutionsinc.store
Downloads  Uploaded photo for ethan.oconnor@techsolutionsinc.store
Music  Uploaded photo for rina.patel@techsolutionsinc.store
PS C:\Users\Amit>
```

The PowerShell window also displays a file explorer sidebar showing various drives and folders, including OneDrive, Desktop, and Downloads.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the Microsoft 365 admin center URL: <https://admin.microsoft.com/#/users/...>. The title bar displays "Amit - 101572711". The main content area shows a user profile for "Julia Martins" with a photo placeholder. Below the photo are three links: "Reset password", "Block sign-in", and "Delete user". A "Change photo" button is also present. The "Account" tab is selected, showing the following details:

Username and email	Aliases
julia.martins@techsolutionsinc.store	Manage username and email
Manage username and email	
Last sign-in	Sign-out i
View last 30 days	Sign this user out of all Microsoft 365 sessions.
Sign out of all sessions	
Alternate email address	Groups
jul*****@techsolutionsinc.store	ARGBC2025
Edit address	TorontoOffice
Manage groups	
Roles	Manager
No administrator access	None provided
Manage roles	Add manager
Contact information	
Display name	First name
Julia Martins	Julia
Phone number	Last name

Here's the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

- o Configure user settings to include organization-specific information.

The screenshot shows a Microsoft Edge browser window with the Microsoft 365 admin center interface. The title bar says 'Amit - 101572711'. The main page is titled 'Manage contact information' and displays the following form fields:

First name	Julia
Last name	Martins
Display name *	Julia Martins
Job title	Marketing Lead
Department	Marketing
Office	101
Office phone	123-555-1001
Fax number	123-555-3001
Mobile phone	123-555-2001
Street address	5 Startup Blvd

At the bottom of the form is a 'Save changes' button.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

Amit -
101572711 //admin.microsoft.com/#/users/-/UserDetails/b326d92f-5abd-49b4-905a-09fb...

Administrator: PowerShell 7 (x64)

```
| Resource '...' does not exist or one of its queried reference-property objects are not present.
```

Status: 404 (NotFound)
ErrorCode: Request_ResourceNotFound
Date: 2025-04-12T23:36:31

Headers:
Last name : Martins
Display name : Julia Martins
Job title : Marketing
Department : Marketing
Office : Office
Office phone : 101
Mobile phone : 123-555-1234
Street address : 5 Startup
City : Toronto

Cache-Control : no-cache
Vary : Accept-Encoding
Strict-Transport-Security : max-age=31536000
request-id : 4b85172f-6430-4683-94bb-5688eca6342a
client-request-id : 4b8a35f-5290-41ca-bdc5-8a22azd34b69
x-ms-ags-diagnostic : {"ServerInfo":{"DataCenter":"Canada Central","Slice":"E","Ring":3,"ScaleUnit":"002","RoleInstance":"T2PEPF00000167"}},
x-ms-resource-unit : 1
Date : Sat, 12 Apr 2025 23:36:31 GMT

Recommendation: See service error codes: <https://learn.microsoft.com/graph/errors>

```
PS C:\Users\Amit> Get-MgUser -All | ForEach-Object {  
>> try {  
>>     Update-MgUser -UserId $_.Id -CompanyName "TechSolutions Inc."  
>>     Write-Host " Updated company name for $($_.UserPrincipalName)"  
>> } catch {  
>>     Write-Warning " Failed to update $($_.UserPrincipalName): $($_.Exception.Message)"  
>> }  
>> }  
>> }
```

Updated company name for 101572711@ARGBC2025.onmicrosoft.com
Updated company name for aisha.chen@techsolutionsinc.store
Updated company name for alice.walker@ARGBC2025.onmicrosoft.com
Updated company name for ARGBC2025@ARGBC2025.onmicrosoft.com
Updated company name for bob.carter@ARGBC2025.onmicrosoft.com
Updated company name for daniel.singh@techsolutionsinc.store
Updated company name for ethan.oconnor@techsolutionsinc.store
Updated company name for Exchange-Admin@ARGBC2025.onmicrosoft.com
Updated company name for fatima.khan@techsolutionsinc.store
Updated company name for GBTESTSHARED1@ARGBC2025.onmicrosoft.com
Updated company name for helpdesk@ARGBC2025.onmicrosoft.com
Updated company name for julia.martins@techsolutionsinc.store
Updated company name for leo.adams@techsolutionsinc.store
Updated company name for malik.carter@techsolutionsinc.store
Updated company name for maria.reyes@techsolutionsinc.store
Updated company name for rina.patel@techsolutionsinc.store
Updated company name for sally@ARGBC2025.onmicrosoft.com
Updated company name for tomasz.novak@techsolutionsinc.store
Updated company name for Toronto@ARGBC2025.onmicrosoft.com
Updated company name for user1@ARGBC2025.onmicrosoft.com
Updated company name for user2@ARGBC2025.onmicrosoft.com

PS C:\Users\Amit>

Zip or postal code: _____
Country or region: _____
Save changes

I also used powershell to update the company name

3. Create Office 365 Groups:

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The title bar displays "Amit - 101572711" and the URL "https://admin.microsoft.com/#/groups". The main header is "Microsoft 365 admin center" with a "Home" link and a "Active groups" breadcrumb. On the left, there's a sidebar with various icons. The main content area is titled "Active groups" and includes links for "About Groups" and "Where to store files". Below this, there are tabs for "Microsoft 365 groups" (which is selected), "Distribution list", and "Security groups". A search bar says "Search all groups". At the top right, there are "Enable Dark mode" and other settings. The main table lists 9 items:

Name	Email	Sync status	Membership type	Primary
All Company	allcompany@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
Amit-G1	assignment1-task4-g1@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
Amit-G2	assignment1-task4-g2@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
ARGBC2025	ARGBC20251515@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
ARGBC2025 - Team Home	ARGBC2025-TeamHome@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Private
HelpDesk	helpdeskGroup@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
Team HQ	TeamHQ@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
TeamVivaldo	TeamVivaldo@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
TorontoOffice	TorontoOffice@ARGBC2025.onmicrosoft.com	Cloud	Dynamic	Public

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, it displays the user's name (Amit - 101572711) and the URL //admin.microsoft.com/#/addgroupwizard/M365Group. The main title is "Add a Microsoft 365 group". On the left, there is a navigation sidebar with various icons and a progress bar indicating the steps: Basics (checkmark), Owners (checkmark), Members (checkmark), Settings (circle), and Finish (circle). The current step is "Owners". The main content area is titled "Assign owners". It explains that group owners have unique permissions and recommends adding two owners. Below this, there is a list of users with checkboxes next to their names: Amit Ratnaparkhi (AR) and helpdesk (H). At the bottom, there are "Back", "Next", and "Cancel" buttons.

I add 2 owners per group (GA and helpdesk)

- Add users to their respective groups.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the URL <https://admin.microsoft.com/#/addgroupwizard/M365Group>. The title bar displays "Amit - 101572711". The main content is the "Microsoft 365 admin center" with the page title "Home > Active groups > Add a Microsoft 365 group". On the left, a navigation pane shows a flowchart with steps: Basics (checked), Owners (checked), Members (checked), Settings (unchecked), and Finish (unchecked). The "Members" step is currently selected. The right panel is titled "Add members" and contains a sub-section titled "Group members have access to everything in the group, including group content like email messages, files, and a shared calendar. By default, group members can invite guests to join your group, but they can't edit group settings." Below this, there is a "Learn more about what group members can do" link. A "Add members" button with a plus sign is present. A list of users is shown with checkboxes next to their names:

- DS Daniel Singh daniel.singh@techsolutionsinc.store
- EO Ethan O'Connor ethan.oconnor@techsolutionsinc.store
- LA Leo Adams leo.adams@techsolutionsinc.store
- MC Malik Carter malik.carter@techsolutionsinc.store
- TN Tomasz Novak tomasz.novak@techsolutionsinc.store

At the bottom, there are "Back", "Next", and "Cancel" buttons, along with a feedback icon.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a navigation bar with tabs like 'Home', 'Active groups', and 'Add a Microsoft 365 group'. A purple sidebar on the left contains icons for Home, Groups, Active Directory, and more. The main content area has a title 'Review and finish adding group' and a sub-instruction 'You're almost there - make sure everything looks right before adding your new group.' Below this, there are sections for 'Group type' (set to 'Microsoft 365'), 'Edit' (link), 'Basics' (Name: IT, Description: IT department, Edit link), 'Owners' (Amit Ratnaparkhi, helpdesk, Edit link), 'Members' (Daniel Singh, Ethan O'Connor, Leo Adams, Malik Carter, Tomasz Novak, Edit link), and 'Settings' (Email: IT@techsolutionsinc.store, Sensitivity: None, Privacy: Private, Role assignment: Disabled, Edit link). At the bottom, there are 'Back', 'Create group' (highlighted in blue), and 'Cancel' buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft 365 Admin Center window titled "Edit settings" for adding a Microsoft 365 group. The left sidebar has a navigation tree with "Basics" (checked), "Owners" (checked), "Members" (checked), "Settings" (selected), and "Finish". The main pane displays settings for a group email address, sensitivity, and privacy. A note at the top says: "You'll be able to change settings, like Allow External Senders or Send Copies of Group Conversations to Members' Inboxes, after the group is created. [Learn more about all settings](#)". Below the note, it says: "Microsoft 365 groups allow teams to collaborate by giving them a group email and a shared workspace for conversations, files, and calendars. Choose settings for your Microsoft 365 group." The "Group email address" field contains "IT @techsolutionsinc.store". The "Sensitivity" dropdown is set to "None". The "Privacy" dropdown is set to "Private". Under "Role assignment", there is a checkbox for "Allow admin roles to be assigned to this group" which is unchecked. A note next to it says: "This setting will be permanent for this group. [Learn more about assigning roles to groups](#)". At the bottom are "Back", "Next", and "Cancel" buttons.

This is the IT department

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a navigation bar with the user name 'Amit - 101572711', a 'Advanced DNS' button, and a search bar. Below the bar, the title 'Microsoft 365 admin center' is displayed, along with a 'Home' link and a 'Enable Dark mode' toggle.

The main content area is titled 'Set up the basics'. It contains a brief description: 'A Microsoft 365 group helps people collaborate. It includes an email address for contacting everyone in the group, and a SharePoint site for publishing information. To get started, fill out some basic info about the group you'd like to create.' Below the description are two input fields: 'Name *' with 'HR' typed in, and 'Description' with 'HR department' typed in. A progress bar on the left indicates the steps: Basics (selected), Owners, Members, Settings, and Finish.

At the bottom right, there are 'Next' and 'Cancel' buttons, and a feedback icon. The overall theme is purple and white, consistent with the Microsoft branding.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the title bar "Amit - 101572711" and the URL "https://admin.microsoft.com/#/addgroupwizard/M365Group". The page is titled "Microsoft 365 admin center" and shows the navigation path "Home > Active groups > Add a Microsoft 365 group". A purple ribbon at the top has icons for Home, Groups, People, Mail, Calendar, Tasks, and More. On the left, a sidebar lists "Basics" (selected), "Owners" (highlighted in blue), "Members", "Settings", and "Finish". The main content area is titled "Assign owners" and contains the following text: "Group owners have unique permissions. They can add or remove members, delete conversations from the shared inbox, and change group settings. Group owners can also rename the group, update the description, and more." A note says "You have to have at least one owner. We recommend adding two, so one can help out in the other's absence." Below this is a section titled "+ Assign owners" with two entries: "Display name" (unchecked) and two user profiles: "Amit Ratnaparkhi" (checked) and "helpdesk" (unchecked). At the bottom are "Back", "Next", and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the URL <https://admin.microsoft.com/#/addgroupwizard/M365Group>. The title bar displays "Amit - 101572711". The main content is the "Microsoft 365 admin center" with the path "Home > Active groups > Add a Microsoft 365 group". A purple navigation bar on the left has icons for Home, Groups, People, Devices, and More. The "Groups" icon is selected. A sidebar on the left shows a flowchart with steps: Basics (checked), Owners (checked), Members (checked), Settings (unchecked), and Finish (unchecked). The main area is titled "Add members". It explains that group members have access to everything in the group, including group content like email messages, files, and a shared calendar. It also states that by default, group members can invite guests to join your group, but they can't edit group settings. Below this, there's a section titled "+ Add members" with checkboxes for "Display name" (unchecked) and two user entries: "Fatima Khan" (checked) and "Maria Reyes" (unchecked). At the bottom are "Back", "Next", and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a navigation bar with the user name 'Amit - 101572711', a tab for 'Advanced DNS', and a search bar. Below the navigation is a purple header bar with the title 'Microsoft 365 admin center' and a link to 'Home > Active groups > Add a Microsoft 365 group'. To the right of the header is a 'Enable Dark mode' button. The main content area has a sidebar on the left with various icons and a vertical ellipsis. On the right, the main panel displays a 'Review and finish adding group' section. It shows a progress flow from 'Basics' to 'Finish', with each step checked off. The 'Finish' step is highlighted with a blue circle. The review section contains the following details:

- Group type:** Microsoft 365 (with an [Edit](#) link)
- Basics:** Name: HR, Description: HR department (with an [Edit](#) link)
- Owners:** Amit Ratnaparkhi, helpdesk (with an [Edit](#) link)
- Members:** Fatima Khan, Maria Reyes (with an [Edit](#) link)
- Settings:** Email: HR@techsolutionsinc.store, Sensitivity: None, Privacy: Private, Role assignment: Disabled (with an [Edit](#) link)

At the bottom of the main panel are buttons for 'Back', 'Create group', and 'Cancel'. There are also small icons for a question mark and a message in the bottom right corner.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a navigation bar with the user name 'Amit - 101572711', a tab for 'Advanced DNS', and a search bar. Below the navigation is a purple header bar with the title 'Microsoft 365 admin center' and a 'Home' button. To the right of the header are icons for search, export, import, notifications, and more, along with a 'Dark mode' toggle.

The main content area is titled 'Edit settings' and displays a wizard for creating a Microsoft 365 group. The left sidebar shows a vertical navigation path: Basics (checked), Owners (checked), Members (checked), Settings (selected), and Finish (unchecked). The right panel contains several configuration fields:

- Group email address ***: A text input field containing 'HR @techsolutionsinc.store'.
- Sensitivity**: A dropdown menu set to 'None'.
- Privacy**: A dropdown menu set to 'Private'.
- Role assignment**: A section with a checkbox labeled 'Allow admin roles to be assigned to this group'. A note below it states: 'This setting will be permanent for this group.' followed by a link 'Learn more about assigning roles to groups'.

At the bottom of the panel are 'Back', 'Next', and 'Cancel' buttons. There are also help and feedback icons in the bottom right corner.

This is the HR department

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the URL <https://admin.microsoft.com/#/addgroupwizard/M365Group>. The title bar displays "Amit - 101572711". The main content is the "Microsoft 365 admin center" with the path "Home > Active groups > Add a Microsoft 365 group". On the left, a sidebar shows navigation icons and a progress bar with steps: Basics (checked), Owners (selected), Members, Settings, and Finish. The right pane is titled "Assign owners" and contains the following text: "Group owners have unique permissions. They can add or remove members, delete conversations from the shared inbox, and change group settings. Group owners can also rename the group, update the description, and more." A note says: "You have to have at least one owner. We recommend adding two, so one can help out in the other's absence." Below this is a section titled "+ Assign owners" with two user entries: "Display name" (unchecked) and "Amit Ratnaparkhi" (checked). The "Next" button is visible at the bottom.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the URL <https://admin.microsoft.com/#/addgroupwizard/M365Group>. The title bar displays "Amit - 101572711". The page is titled "Add members" under the heading "Add a Microsoft 365 group". A sidebar on the left shows a navigation tree with "Basics" (checked), "Owners" (checked), "Members" (checked), "Settings" (unchecked), and "Finish" (unchecked). The main content area contains a sub-section titled "Add members" with a note explaining that group members have access to everything in the group, including group content like email messages, files, and a shared calendar. It also links to "Learn more about what group members can do". Below this, there is a list of users with checkboxes next to their names: Aisha Chen (aisha.chen@techsolutionsinc.store), Julia Martins (julia.martins@techsolutionsinc.store), and Rina Patel (rina.patel@techsolutionsinc.store). At the bottom of the page are "Back", "Next", and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the URL <https://admin.microsoft.com/#/addgroupwizard/M365Group>. The title bar displays "Amit - 101572711". The main content is the "Edit settings" page for creating a Microsoft 365 group. On the left, a vertical navigation pane shows a progress bar with steps: Basics (checked), Owners (checked), Members (checked), Settings (selected), and Finish (unchecked). The right pane contains the following fields:

- Group email address ***: marketing @techsolutionsinc.store
- Sensitivity**: None
- Privacy**: Private
- Role assignment**: A checkbox labeled "Allow admin roles to be assigned to this group" is unchecked. Below it, a note states: "This setting will be permanent for this group. [Learn more about assigning roles to groups](#)".

At the bottom are "Back", "Next", and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a navigation bar with the user name 'Amit - 101572711', a tab for 'Advanced DNS', and a search bar. Below the navigation is a purple header bar with the title 'Microsoft 365 admin center'. The main content area has a left sidebar with various icons and a vertical navigation menu. The main panel displays a 'Review and finish adding group' section. On the left, a vertical flowchart shows five steps: Basics (checked), Owners (checked), Members (checked), Settings (checked), and Finish (highlighted). To the right, the 'Review and finish adding group' section contains the following details:

- Group type:** Microsoft 365. [Edit](#)
- Basics:** Name: Marketing, Description: Marketing department. [Edit](#)
- Owners:** Amit Ratnaparkhi, helpdesk. [Edit](#)
- Members:** Aisha Chen, Julia Martins, Rina Patel. [Edit](#)
- Settings:** Email: marketing@techsolutionsinc.store, Sensitivity: None, Privacy: Private, Role assignment: Disabled. [Edit](#)

At the bottom of the review section are buttons for 'Back', 'Create group', and 'Cancel'.

This is the marketing department

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 admin center interface. The top navigation bar includes the user name 'Amit - 101572711', the 'Advanced DNS' status, and a search bar. The main header says 'Microsoft 365 admin center'. On the left, there's a sidebar with various icons. The main content area is titled 'Microsoft 365 groups' and displays a list of 12 items. The columns in the list are 'Name ↑', 'Email', 'Sync status', 'Membership type', and 'Pri'. The items listed are:

Name ↑	Email	Sync status	Membership type	Pri
All Company	allcompany@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
Amit-G1	assignment2-task4-g1@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
Amit-G2	assignment2-task4-g2@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
ARGBC2025	ARGBC20251515@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
ARGBC2025 - Team Home	ARGBC2025-TeamHome@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Private
HelpDesk	helpdeskGroup@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
HR	HR@techsolutionsinc.store	Cloud	Assigned	Private
IT	IT@techsolutionsinc.store	Cloud	Assigned	Private
Marketing	marketing@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Private
Team HQ	TeamHQ@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
TeamVivaldo	TeamVivaldo@ARGBC2025.onmicrosoft.com	Cloud	Assigned	Public
TorontoOffice	TorontoOffice@ARGBC2025.onmicrosoft.com	Cloud	Dynamic	Private

Confirmation of groups creation

4. Configure User Permissions:

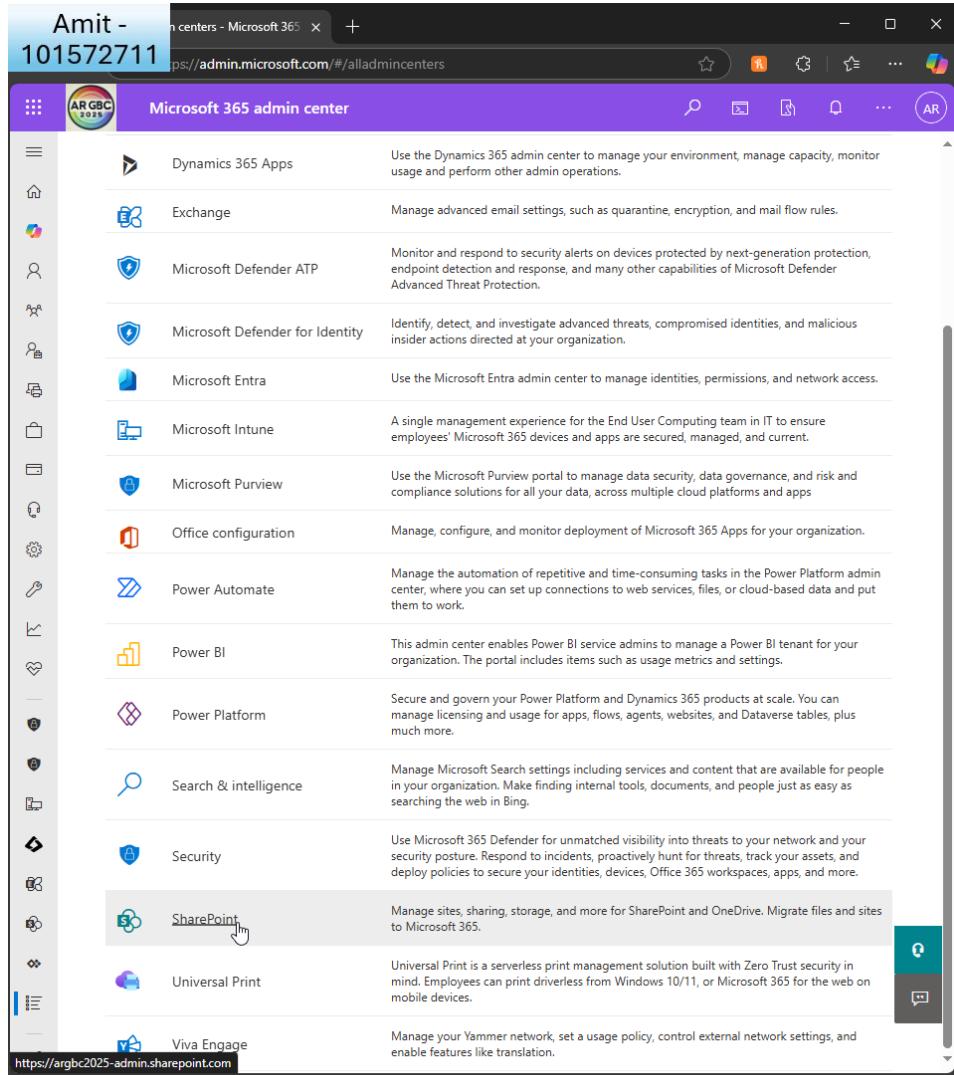
Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

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



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a vertical list of icons corresponding to various admin centers. The 'SharePoint' icon is highlighted with a mouse cursor, indicating it is the target of the assignment task. The main content area lists several admin centers with their descriptions:

Admin Center	Description
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.
Security	Use Microsoft 365 Defender for unmatched visibility into threats to your network and your security posture. Respond to incidents, proactively hunt for threats, track your assets, and deploy policies to secure your identities, devices, Office 365 workspaces, apps, and more.
SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
Universal Print	Universal Print is a serverless print management solution built with Zero Trust security in mind. Employees can print driverless from Windows 10/11, or Microsoft 365 for the web on mobile devices.
Viva Engage	Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the SharePoint Admin Center interface. The left sidebar has a navigation menu with items like Home, Sites, Active sites (which is selected), Deleted sites, Containers, Policies, Settings, Content services, Migration, Reports, More features, Advanced management (PRO), Customize navigation, and Show all. The main content area is titled "Active sites" and displays a table of sites. The table has columns for Site name, URL, and Teams. The "Site name" column is sorted by ascending order. The table lists several sites, with "HR" being highlighted with a blue checkmark and a gray background. Other sites listed include All Company, Amit-G1, Amit-G2, ARGBC2025 - Sharepoint - Ho..., ARGBC2025 - Team Home, Communication site, Communications HQ, HelpDesk, IT, Marketing, Team HQ, TeamVivaldo, and TorontoOffice. A progress bar at the top right indicates "1.24 TB available of 1.24 TB". A search bar at the top right contains the text "Search sites".

Site name ↑	URL	Teams
All Company	.../sites/allcompany	-
Amit-G1	.../sites/assignment2-task4	-
Amit-G2	.../sites/assignment2-task4-g2	-
ARGBC2025 - Sharepoint - Ho...	.../sites/ARGBC2025-Sharepoint-Ho...	-
ARGBC2025 - Team Home	.../sites/ARGBC2025-TeamHome	-
Communication site	https://argbc2025.sharepoint.com	-
Communications HQ	.../sites/CommunicationsHQ	-
HelpDesk	.../sites/helpdeskGroup	-
HR	.../sites/HR	-
IT	.../sites/IT	-
Marketing	.../sites/marketing	-
Team HQ	.../sites/TeamHQ	-
TeamVivaldo	.../sites/TeamVivaldo	-
TorontoOffice	.../sites/TorontoOffice	-

I choose the HR sharepoint site

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the URL https://argbc2025-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/site.... The title bar displays "Amit - 101572711". The SharePoint Admin Center ribbon has "SharePoint admin center" selected. A navigation bar on the left lists "General", "Activity", "Membership" (which is underlined), and "Settings". The main content area shows a group named "HR" (Private group). It includes options to "Email", "View site", and "Delete". Below the group name is the description "HR department". A sidebar on the left lists "Owners", "Members" (which is selected and highlighted in grey), "Site admins", "Site owners", "Site members", "Site visitors", and "About membership and permissions". The "Members" section shows two users: Fatima Khan (FK) and Maria Reyes (MR). Each user has a checkbox next to their name and an email address listed. There is also a search bar labeled "Search all members...".

I see the members of the group

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint site named 'HR'. The browser tabs are 'Active sites - SharePoint admin center' and 'HR - Home'. The address bar shows the URL <https://argbc2025.sharepoint.com/sites/HR>. The page header includes the SharePoint logo, a search bar, and a settings icon. The main content area displays a news section with a placeholder image of a tablet and a potted plant, and an activity feed showing two posts: one from 'HR +1' and one from 'HR Owners'. A sidebar on the right is titled 'Settings' and contains links for SharePoint management, including 'Add a page', 'Site contents', 'Site information', 'Site permissions', 'Apply a site template', 'Site usage', 'Site performance', 'Change the look', and 'Site branding (new)'. Below this is a 'Microsoft 365' section with a 'View all' link.

I change site permissions

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint site titled "HR". The page includes a news section with a post about a new group being ready, and an activity section showing recent posts from site owners. On the right, a "Permissions" dialog box is open, showing Site Owners with full control, Site members with limited control, and Site visitors with no control. It also includes sections for Site Sharing and Guest Expiration, with a link to "Advanced permissions settings" highlighted by a mouse cursor.

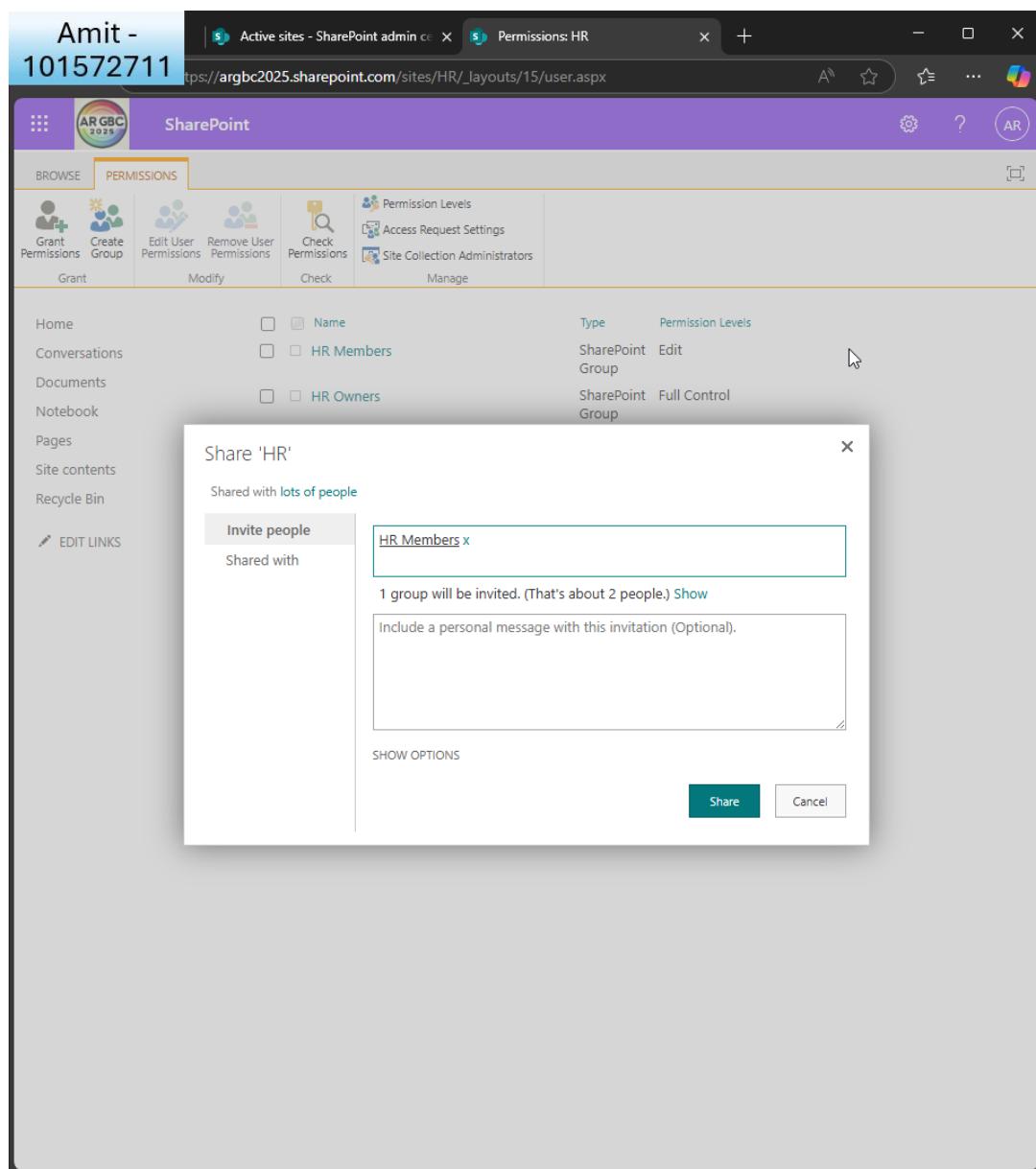
I click 'advanced permissions settings'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I choose HR group

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the title bar "Amit - 101572711" and the address bar "https://argbc2025.sharepoint.com/sites/HR/_layouts/15/user.aspx". The SharePoint ribbon has "SharePoint" selected. The "PERMISSIONS" tab is active. Below the ribbon, there are four main sections: "Grant" (with "Grant Permissions" and "Create Group" buttons), "Modify" (with "Edit User Permissions" and "Remove User Permissions" buttons), "Check" (with "Check Permissions" button), and "Manage" (with "Permission Levels", "Access Request Settings", and "Site Collection Administrators" buttons). The main content area displays a table of permissions for the "HR" group:

	Type	Permission Levels
Home	<input type="checkbox"/> <input checked="" type="checkbox"/> Name	SharePoint Edit
Conversations	<input type="checkbox"/> <input checked="" type="checkbox"/> HR Members	Group
Documents	<input type="checkbox"/> <input checked="" type="checkbox"/> HR Owners	SharePoint Full Control
Notebook		Group
Pages	<input type="checkbox"/> <input checked="" type="checkbox"/> HR Visitors	SharePoint Read
Site contents		Group
Recycle Bin		

At the bottom left, there is a "EDIT LINKS" button.

I can see the different levels of permissions

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface. The title bar displays "Amit - 101572711" and "Microsoft 365 admin center". The left sidebar has a "Security" icon highlighted with a blue box. The main content area is titled "Active users" and lists user accounts with columns for "Display name ↑", "Username", and "Licenses". A search bar at the top right says "Search active users list".

Display name ↑	Username	Licenses
101572711	101572711@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Aisha Chen	aisha.chen@techsolutionsinc.store	Microsoft 365 E5 (no Team)
Alice Walker	alice.walker@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Amit Ratnaparkhi	ARGBC2025@ARGBC2025.onmicrosoft.com	Microsoft Power Apps for Automate Free , Microsoft
Bob Carter	bob.carter@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Daniel Singh	daniel.singh@techsolutionsinc.store	Microsoft 365 E5 (no Team)
dynamicUser1	dynamicUser1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Ethan O'Connor	ethan.oconnor@techsolutionsinc.store	Microsoft 365 E5 (no Team)
Exchange-Admin	Exchange-Admin@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Fatima Khan	fatima.khan@techsolutionsinc.store	Microsoft 365 E5 (no Team)
GBTTESTSHARED1	GBTTESTSHARED1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
helpdesk	helpdesk@ARGBC2025.onmicrosoft.com	Microsoft 365 E5
Julia Martins	julia.martins@techsolutionsinc.store	Microsoft 365 E5
Leo Adams	leo.adams@techsolutionsinc.store	Microsoft 365 E5 (no Team)

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender Home page. At the top left, it displays "Amit - 101572711". The top right shows "Home - Microsoft Defender" and a search bar. Below the header is a sidebar with various navigation options: Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface (with Map and Attack paths), Exposure insights, Secure score (which is highlighted with a cursor), Data connectors, Assets, Devices, Identities, Applications, and Endpoints. The main content area is titled "Home" and features a banner with the text "Get your SIEM and XDR in one place" and a "Connect a workspace" button. Below the banner is a "Microsoft Secure Score" section. It shows a secure score of "Secure score: cure Score: 50.5%" and "196.45/389 points achieved". It also includes a chart titled "Identity" with a value of "82.63" and a timeline from "03/24" to "04/12". At the bottom of the page, the URL "https://security.microsoft.com/exposure-secure-score?tid=c891450f-9cdc-42f0-9b88-0928b661f..." is visible.

Here I can see my score of 50.5%

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface with the title "Amit - 101572711". The left sidebar lists various security categories: Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface (Map, Attack paths), Exposure insights, Secure score (selected), Data connectors, Assets, Devices, Identities, Applications, Endpoints, and Vulnerability management. The main area displays the "Microsoft Secure Score" dashboard with a dark background featuring a lock and a shield icon. Below the dashboard, a section titled "Recommended actions" is shown, with the sub-tab "Recommended actions" being active. It lists 99 items and provides a table of 10 recommended actions:

Rank	Recommended action	Score
1	Ensure that intelligence for impersonation protection is enabled	+2
2	Move messages that are detected as impersonated users by mail	+2
3	Enable impersonated domain protection	+2
4	Set the phishing email level threshold at 2 or higher	+2
5	Enable impersonated user protection	+2
6	Ensure 'Phishing-resistant MFA strength' is required for Admin	+1
7	Quarantine messages that are detected from impersonated do	+1
8	Quarantine messages that are detected from impersonated use	+1
9	Ensure password protection is enabled for on-prem Active Dire	+1
10	Start your Defender for Identity deployment, installing Sensors	+1

Here I see a list of recommendations

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Secure Score dashboard. At the top, there's a navigation bar with a user profile (Amit - 101572711), a search bar, and various icons. Below the bar, there's a decorative graphic of a lock and a compass. The main title is "Microsoft Secure Score". Below the title, there are four tabs: "Overview", "Recommended actions" (which is underlined in blue, indicating it's active), "History", and "Metrics & trends". A sub-section titled "Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours." is displayed. It includes an "Export" button, a search bar, and a table of 99 items. The table has columns for "Rank", "Recommended action", and "Score". The first few items in the list are:

Rank	Recommended action	Score
1	Ensure that intelligence for impersonation protection is enabled	+2
2	Move messages that are detected as impersonated users by mail	+2
3	Enable impersonated domain protection	+2
4	Set the phishing email level threshold at 2 or higher	+2
5	Enable impersonated user protection	+2
6	Ensure 'Phishing-resistant MFA strength' is required for Admin	+1
7	Quarantine messages that are detected from impersonated do	+1
8	Quarantine messages that are detected from impersonated use	+1
9	Ensure password protection is enabled for on-prem Active Dire	+1
10	Start your Defender for Identity deployment, installing Sensors	+1

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for managing security policies. The left sidebar contains a navigation menu with categories like Partners and APIs, Configuration management, Identities, Service accounts, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, and Policies & rules. The Policies & rules section is currently selected. The main content area is titled "Policies & rules" and includes a sub-section for "Threat policies". A callout box highlights the "Threat policies" link, which is underlined in blue. Below this, there are links for "Alert policy" and "Activity alerts". A status bar at the bottom indicates "3 items".

I check the current threat policies

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for managing safe links. The left sidebar has a dark theme with various sections like Partners and APIs, Configuration management, Identities, Service accounts, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Activity log, and Governance log. The main pane is titled "Safe links" and displays a message about enabling preset security policies. Below is a table with one item:

Name	Status	Priority
Built-in protection (Microsoft)	On	Lowest

I can see safe links is already enabled

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for managing safe attachments. The left sidebar lists various security categories like Partners and APIs, Configuration management, Identities, Service accounts, Health issues, Tools, Email & collaboration, Cloud apps, and Policies & rules. The main content area is titled "Safe attachments" and displays a single item: "Built-in protection (Microsoft)" which is set to "On". A note at the top encourages enabling preset security policies.

Name	Status	Priority
Built-in protection (Microsoft)	On	Lowest

As is safe attachments

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for managing anti-phishing policies. The left sidebar lists various categories like Partners and APIs, Configuration management, Identities, Service accounts, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Activity log, and Governance log. The main content area is titled "Anti-phishing" and contains a brief description of built-in protection features. It includes a callout for enabling preset security policies and a status bar indicating 0 impersonated domain(s) and user(s) over the past 7 days. A table lists the current policy, showing "Office365 AntiPhish Default (De...)" with a green "Always on" status indicator and "Lowest" priority.

Name	Status	Priority	Last modified
Office365 AntiPhish Default (De...)	Always on	Lowest	Apr 12, 2024

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Defender interface for creating a new anti-phishing policy. The left sidebar lists steps: Policy name (checked), Users, groups, and domains (selected), Phishing threshold & protection, Actions, and Review. The main area is titled "Users, groups, and domains" and contains fields for "Include these users, groups and domains *". Under "Groups", "HR" is listed. Under "Domains", "techsolutionsinc.store" is listed. A checkbox for "Exclude these users, groups and domains" is present but unchecked. At the bottom are "Back", "Next", and "Cancel" buttons.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Defender interface for creating a new anti-phishing policy. The left sidebar lists steps: Policy name (checked), Users, groups, and domains (checked), Phishing threshold & protection (selected), Actions (unchecked), and Review (unchecked). The main panel is titled "Phishing threshold & protection". It includes a note about setting thresholds and protections. A slider for "Phishing email threshold" is set to "3 - More Aggressive". Below the slider, it says messages are treated as if identified with a very high degree of confidence. Under "Impersonation", there's a note about 0 impersonation emails detected in the last 7 days, a checkbox for enabling users to protect (0/350), and a link to learn more about adding users to impersonation protection. There's also a section for managing sender domains. At the bottom are "Back", "Next", and "Cancel" buttons.

I choose a more aggressive threshold

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Defender interface for creating a new anti-phishing policy. The left sidebar lists steps: Policy name (checked), Users, groups, and domains (checked), Phishing threshold & protection (checked), Actions (selected), and Review (unchecked). The main pane details policy actions based on message detection:

- If a message is detected as user impersonation: Don't apply any action
- If a message is detected as domain impersonation: Don't apply any action
- If Mailbox Intelligence detects an impersonated user: Don't apply any action
- Honor DMARC record policy when the message is detected as spoof
- If the message is detected as spoof and DMARC Policy is set as p=quarantine: Quarantine the message

We'll quarantine the message for you to review and decide whether it should be released. [Learn how to manage quarantined messages](#)

- If the message is detected as spoof and DMARC Policy is set as p=reject: Reject the message

Reject the message so it won't be delivered

- If the message is detected as spoof by spoof intelligence: Move the message to the recipients' Junk Email folders

Move the message to the recipients' Junk Email folders

Safety tips & indicators ⓘ

- Show first contact safety tip (Recommended) ⓘ
- Show (?) for unauthenticated senders for spoof ⓘ

Buttons at the bottom: Back, Next, Cancel.

I keep default settings

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Defender interface for creating a new anti-phishing policy. On the left, a vertical checklist indicates the steps completed: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The 'Review' step is highlighted with a blue circle. The main pane displays the policy details under the heading 'Review'. It includes sections for Policy name (Anti Phishing), Users, groups, and domains (Included groups: HR@techsolutionsinc.store, Included recipient domains: techsolutionsinc.store), Phishing threshold and protections (3 - More Aggressive), User impersonation protection (Off - 0 sender(s) specified), Domain impersonation protection (Off for owned domains, Off - 0 domain(s) specified), Trusted impersonated senders and domains (Off), Mailbox intelligence (On), and Mailbox intelligence for impersonations. At the bottom are 'Back', 'Submit' (highlighted in blue), and 'Cancel' buttons.

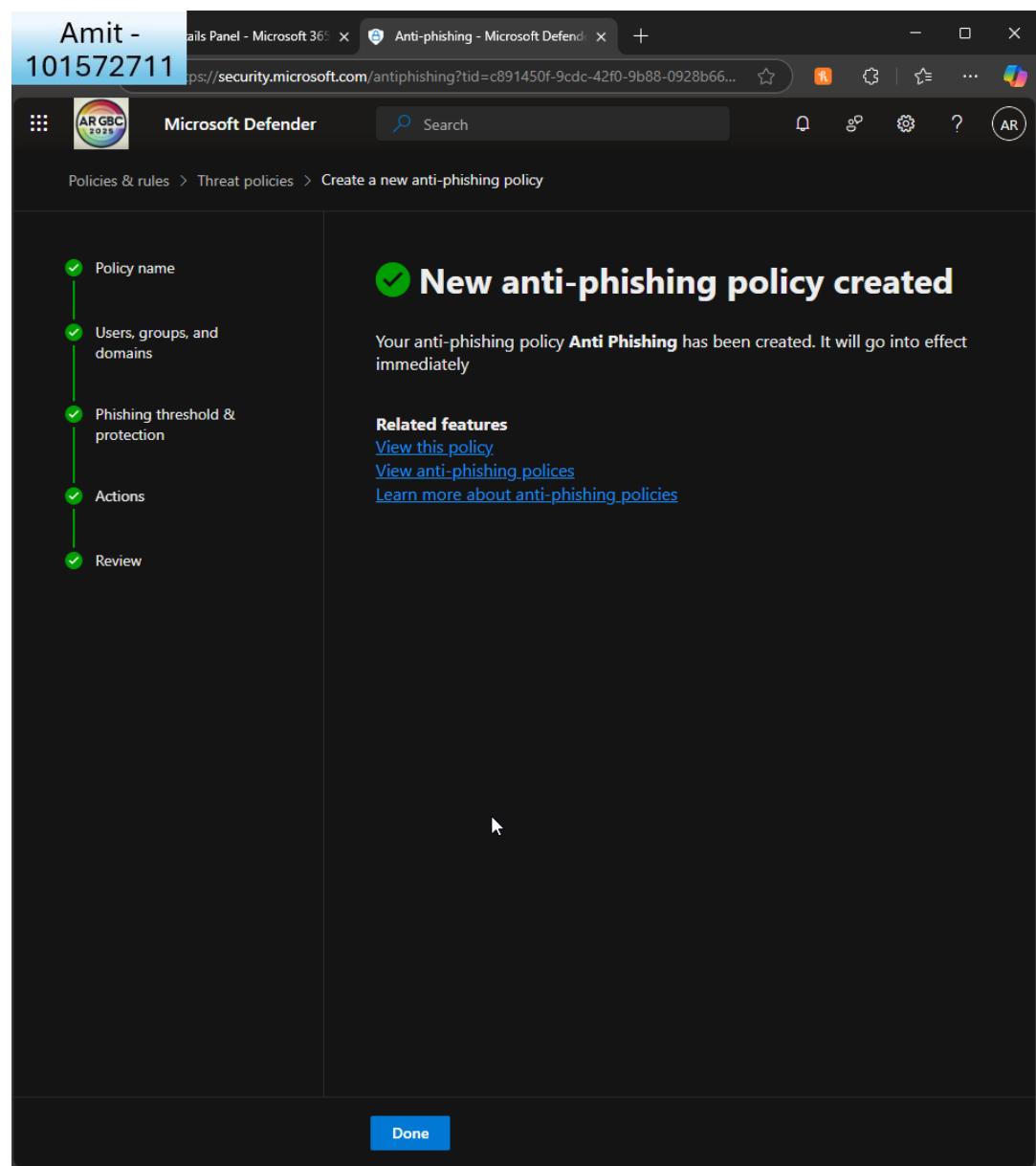
I review the policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

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)

The screenshot shows the Microsoft 365 Admin Center interface. The top navigation bar includes the user name 'Amit - 101572711', the URL 'https://admin.microsoft.com/#/alladmincenters', and a 'Microsoft 365 admin center' title. On the left is a vertical sidebar with various icons representing different admin centers. The main content area is titled 'All admin centers' and lists ten available admin centers with their names and descriptions. The 'Exchange' center is highlighted with a light gray background. At the bottom of the page, there is a footer with the URL 'https://admin.exchange.microsoft.com/?landingpage=h...' and a note about using Microsoft 365 Defender for unmatched visibility into threats.

Name	Description
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Exchange Admin Center interface. At the top left, it displays "Amit - 101572711". The top navigation bar includes links for "Home centers - Microsoft 365", "Exchange admin center", and a search bar. On the far right of the top bar are icons for "Add card (5 more available)", "What's new?", "Dark mode", and a user profile icon.

The left sidebar contains a navigation menu with the following items:

- Home
- Recipients
- Mailboxes
- Groups
- Resources
- Contacts
- Mail flow
- Message trace
- Rules** (highlighted with a cursor icon)
- Remote domains
- Accepted domains
- Connectors
- High Volume Email (Preview)
- Alerts
- Alert policies
- Roles
- Migration
- Mobile
- Reports
- Insights
- Public folders
- Organization
- Settings
- Troubleshoot
- Other features

The main content area features a banner titled "More Secure, Reliable REST Backed EXO Cmdlets" with the sub-section "Exchange Online New REST Module". It includes a note about REST backed PowerShell cmdlets being released, a "Click here to know more" button, and sections for "Training & guides" (with "Training for admins" and "Documentation" links) and "Mailboxes" (with "Manage email forwarding", "Add a shared mailbox", "Hide from address list", and "Edit a mailbox" options). A vertical sidebar on the right contains a "Help" icon and a "Feedback" icon.

I click 'rules' in Exchange admin centre

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Exchange Admin Center interface. The top navigation bar includes the user name 'Amit - 101572711', the title 'Exchange admin center', and a search bar. A banner at the top right informs users that DLP policies and conditions are no longer supported and should be migrated to Microsoft Purview DLP. The left sidebar has a 'Mail flow' section selected, which includes 'Rules' (highlighted in blue), 'Remote domains', 'Accepted domains', 'Connectors', 'High Volume Email (Preview)', 'Alerts', and 'Alert policies'. Below this are sections for 'Roles', 'Migration', 'Mobile', 'Reports', 'Insights', 'Public folders', 'Organization', 'Settings', 'Troubleshoot', and 'Other features'. The main content area is titled 'Rules' and contains a sub-header 'Add, edit, or make other changes to your transport rules.' It features a 'Create a new rule' input field and a list of actions: 'Apply Office 365 Message Encryption and rights protection to messages', 'Apply custom branding to OME messages', 'Apply disclaimers', 'Filter messages by size', 'Modify messages', 'Restrict managers and their direct reports', 'Restrict messages by sender or recipient', 'Send messages to a moderator', and 'Send messages and save a copy for review'. A 'Dark mode' toggle is visible in the top right corner.

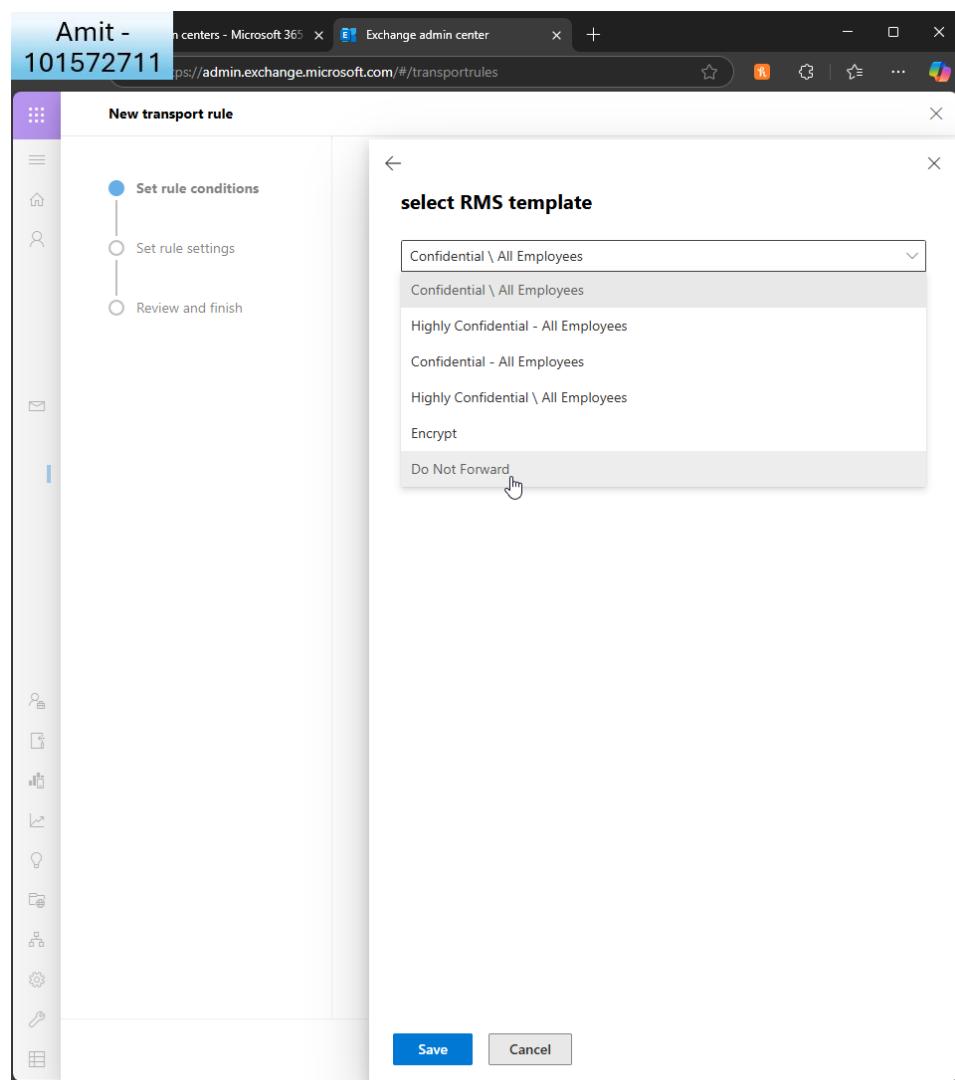
I create a new rule

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



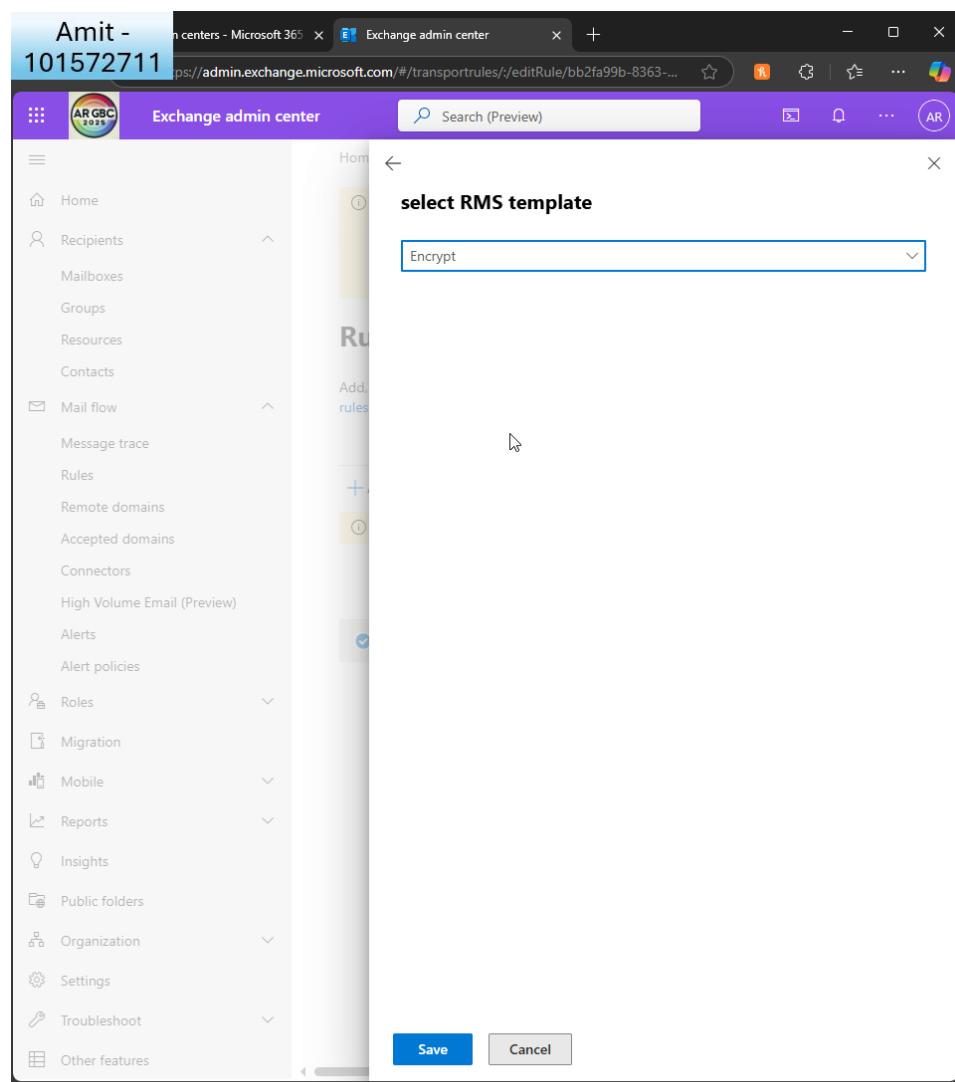
I set it so it doesn't forward (then changed it to 'encrypt' as per assignment rules - below)

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

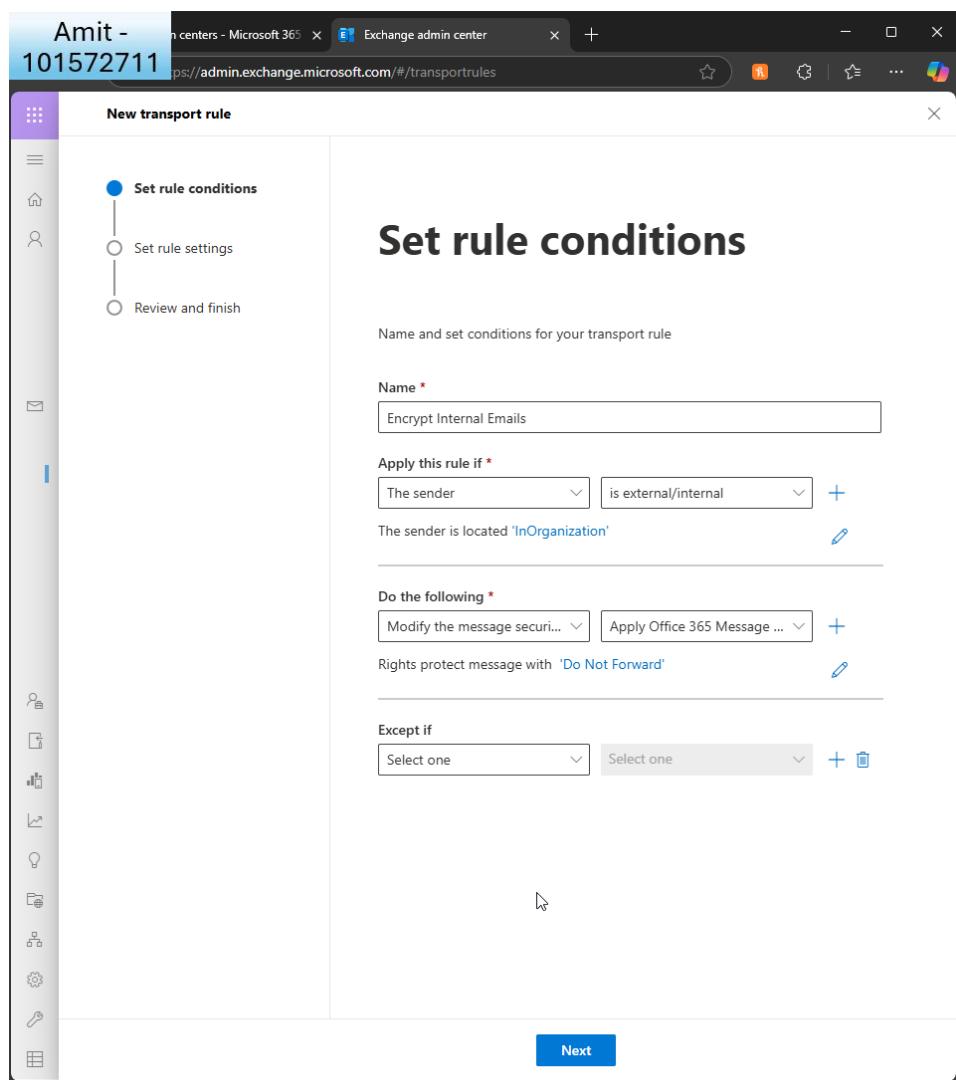


Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

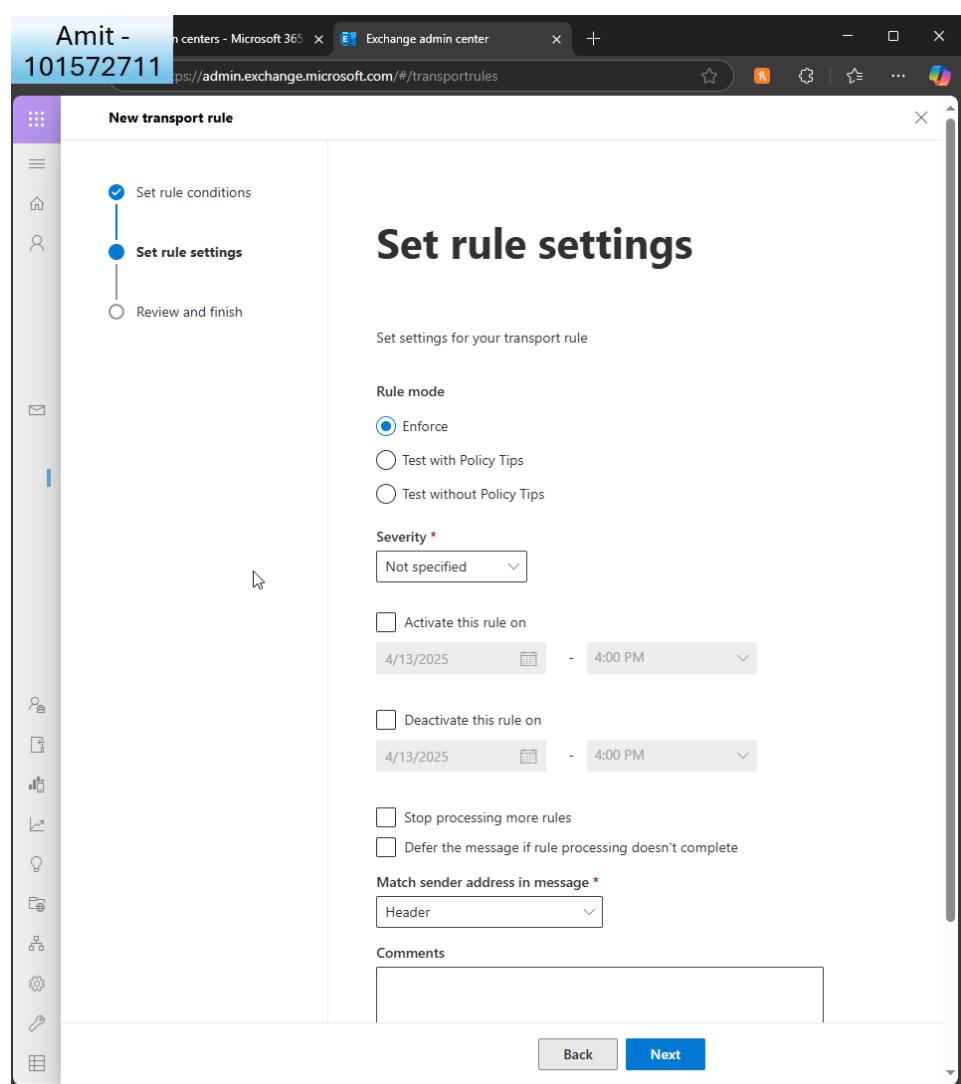


I set the conditions so if the sender is inside the organisation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



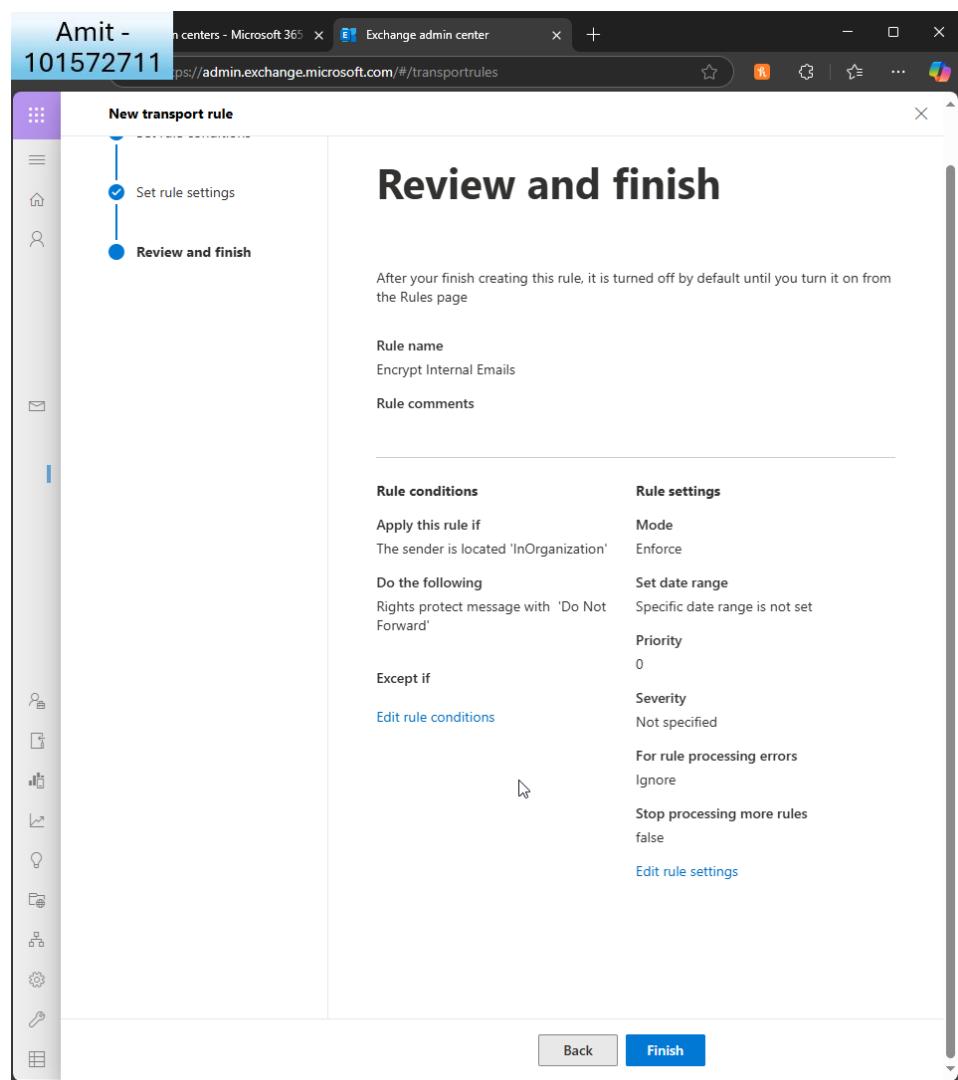
I enforce the policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



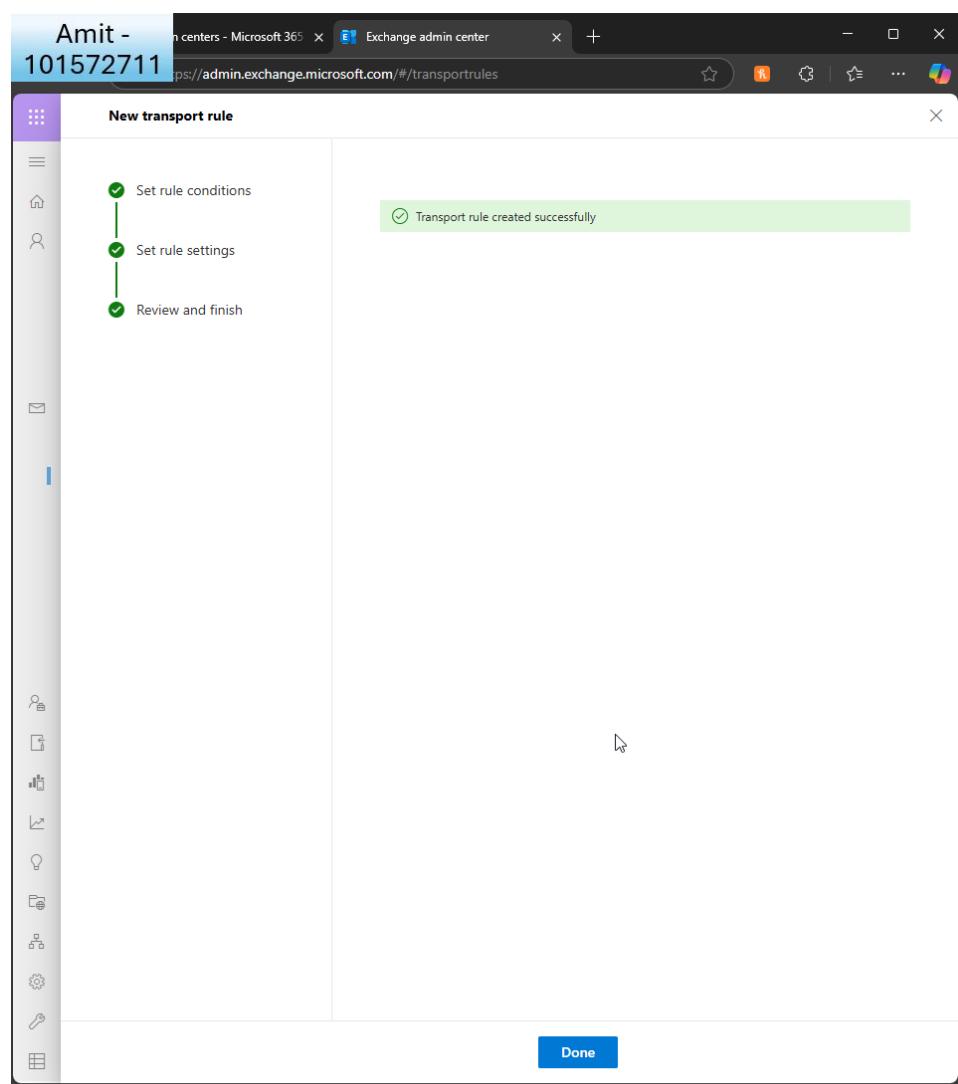
I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Exchange admin center interface. The left sidebar lists various administrative categories like Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow, Message trace, Rules, Remote domains, Accepted domains, Connectors, High Volume Email (Preview), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, Settings, Troubleshoot, and Other features. The main content area is titled 'Encrypt Internal Emails'. It displays the status as 'Disabled' and has a toggle switch set to 'Enabled'. A progress bar indicates 'Updating the rule status, please wait...'. Below this, there are sections for 'Rule settings' (Rule name: Encrypt Internal Emails, Mode: Enforce, Severity: Not specified, Set date range: Specific date range is not set, Senders address: Matching Header, Priority: 0) and 'Rule description' (Apply this rule if: Is received from 'Inside the organization', Do the following: rights protect message with RMS template: 'Do Not Forward').

I enable the rule

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Exchange Admin Center interface. The left sidebar has a 'Mail flow' section with 'Rules' selected. The main area is titled 'Rules' and contains a table with one row. The table columns are Status, Rule, Priority, Stop pr..., Size (By...), and Last ex... . The single row shows: Enabled, Encrypt Internal Emails, 0, X, 472. There is a yellow banner at the top right stating: 'DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be created or edited in the Exchange Admin Center (EAC) or using Exchange Online PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center as soon as possible. Once you have migrated these rules please delete them here in the EAC or via PowerShell. Learn more: Migrate DLP policies | No DLP-conditions or actions'.

Status	Rule	Priority	Stop pr...	Size (By...)	Last ex...
Enabled	Encrypt Internal Emails	0	X	472	

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.

Microsoft 365 Identity and Services – Enterprise Administration

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!

Microsoft 365 Identity and Services – Enterprise Administration

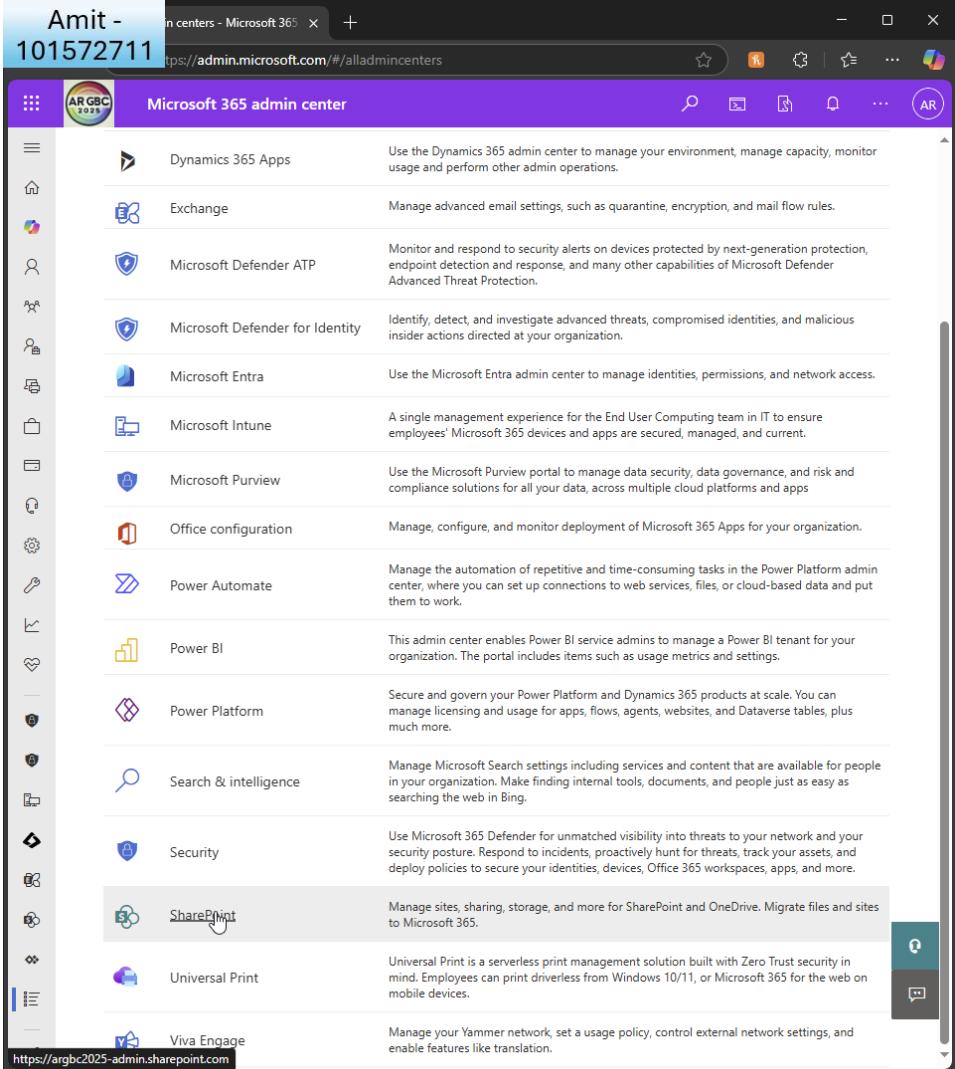
Student Name:
Student ID:

Term:

Task 3: Configuring and Managing Collaboration Tools

1. Set Up SharePoint Online:

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



The screenshot shows the Microsoft 365 Admin Center interface. On the left is a vertical navigation bar with various icons. The main area lists several administrative tools. The 'SharePoint' link is highlighted with a blue box, indicating it is the target for configuration. Other listed tools include Dynamics 365 Apps, Exchange, Microsoft Defender ATP, Microsoft Defender for Identity, Microsoft Entra, Microsoft Intune, Microsoft Purview, Office configuration, Power Automate, Power BI, Power Platform, Search & intelligence, Security, Universal Print, and Viva Engage.

Link	Description
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.
Security	Use Microsoft 365 Defender for unmatched visibility into threats to your network and your security posture. Respond to incidents, proactively hunt for threats, track your assets, and deploy policies to secure your identities, devices, Office 365 workspaces, apps, and more.
SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
Universal Print	Universal Print is a serverless print management solution built with Zero Trust security in mind. Employees can print driverless from Windows 10/11, or Microsoft 365 for the web on mobile devices.
Viva Engage	Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the SharePoint Admin Center interface. The left sidebar has a navigation menu with items like Home, Sites (Active sites selected), Deleted sites, Containers, Policies, Settings, Content services, Migration, Reports, More features, Advanced management (PRO), Customize navigation, and Show all. The main content area is titled "Active sites" and displays a table of sites. The table has columns for Site name, URL, and Teams. There are 18 rows listed, including All Company, Amit-G1, Amit-G2, ARGBC2025 - Sharepoint - Ho..., ARGBC2025 - Team Home, Communication site, Communications HQ, HelpDesk, HR, IT, Marketing, Team HQ, TeamVivaldo, and TorontoOffice. The rows for HR, IT, and Marketing are highlighted with a blue background and have a checkmark icon to their left. A search bar at the top right says "Search sites" and shows "3 selected". A progress bar at the top right indicates "1.24 TB available of 1.24 TB".

Site name ↑	URL	Teams
All Company	.../sites/allcompany	-
Amit-G1	.../sites/assignment2-task4	-
Amit-G2	.../sites/assignment2-task4-g2	-
ARGBC2025 - Sharepoint - Ho...	.../sites/ARGBC2025-Sharepoint-Ho...	-
ARGBC2025 - Team Home	.../sites/ARGBC2025-TeamHome	-
Communication site	https://argbc2025.sharepoint.com	-
Communications HQ	.../sites/CommunicationsHQ	-
HelpDesk	.../sites/helpdeskGroup	-
<input checked="" type="checkbox"/> HR	.../sites/HR	-
<input checked="" type="checkbox"/> IT	.../sites/IT	-
<input checked="" type="checkbox"/> Marketing	.../sites/marketing	-
Team HQ	.../sites/TeamHQ	-
TeamVivaldo	.../sites/TeamVivaldo	-
TorontoOffice	.../sites/TorontoOffice	-

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the URL https://argbc2025-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/site.... The title bar displays "Amit - 101572711" and the SharePoint admin center logo. The page content shows a team named "HR" which is a "Private group". Below the team name are links for "Email", "View site", and "Delete". A sub-section titled "HR department" is visible. At the top of the main content area are tabs: General, Activity, Membership, and Settings, with Settings being the active tab. Under the Settings tab, there are several configuration sections: "Email" (with checkboxes for letting people outside the organization email the team, sending copies of emails to members' inboxes, and hiding the team's email address in Outlook), "Privacy" (set to Private), "External file sharing" (set to New and existing guests), "Sensitivity label" (set to None), "Custom scripts" (Blocked, Edit link), and "Version history limit" (Same as Organization-level (Manual)). A "Save" button is located at the bottom left.

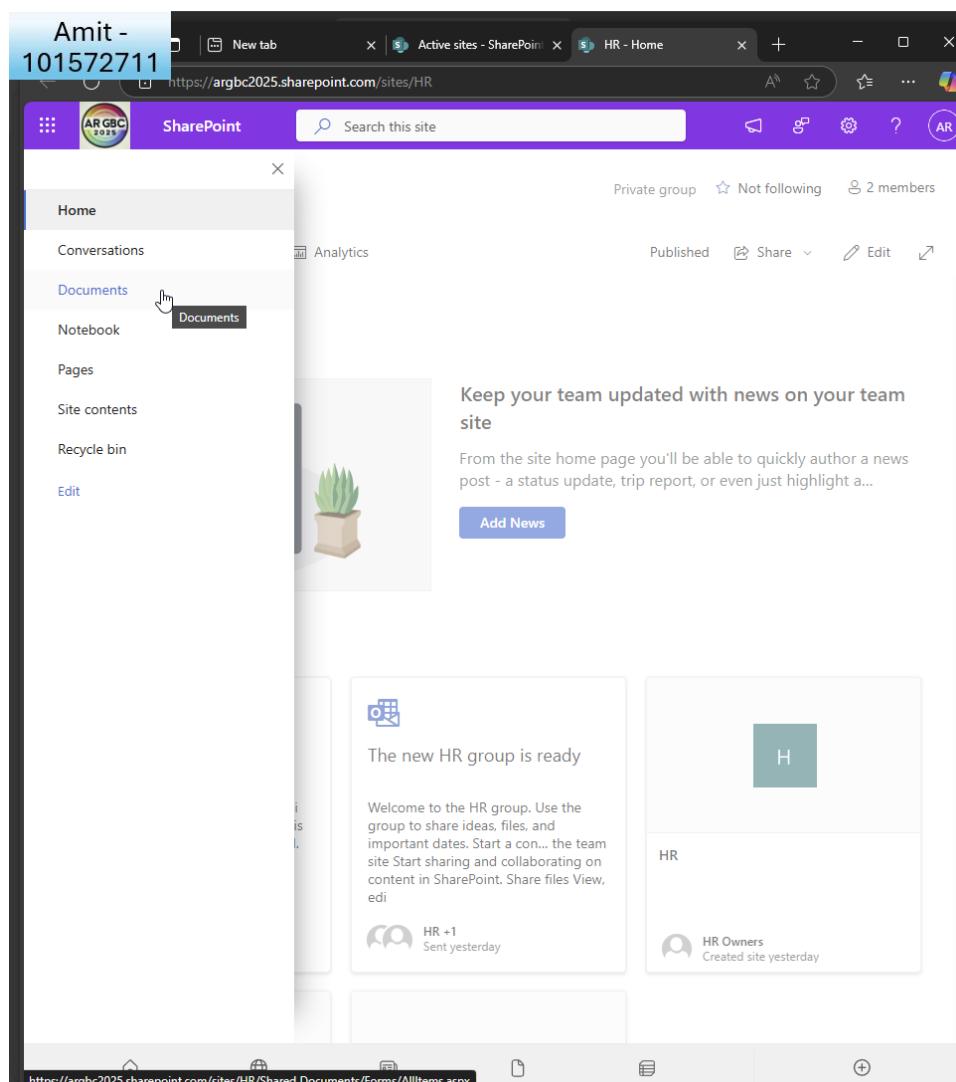
HR site

- Configure document libraries and permissions for each site.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

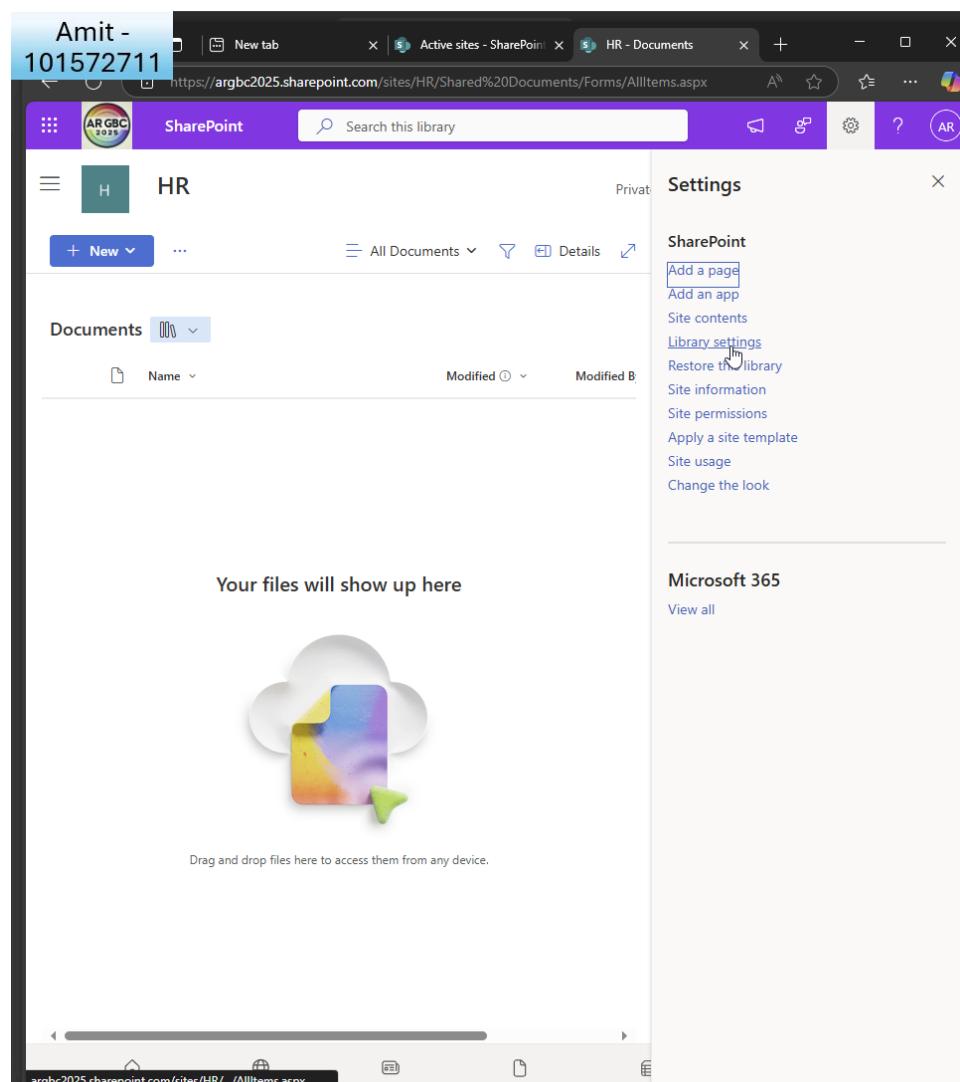


Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I click library settings within documents of the sharepoint site

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft SharePoint interface. At the top, there's a navigation bar with links like Home, Conversations, Documents, Notebook, Pages, Site contents, and Recycle Bin. On the left, there's a sidebar with 'EDIT LINKS' and a list of items including Home, Conversations, Documents, Notebook, Pages, Site contents, and Recycle Bin. The main content area is titled 'Documents > Settings'. It displays 'List Information' with fields for Name (Documents), Web Address (https://argbc2025.sharepoint.com/sites/HR/_layouts/15/user.aspx?obj=%7B9DB03D15-7810-4CBB-...), and Description. Below this are three tabs: General Settings, Permissions and Management, and Communications. Under General Settings, there are several sections with expandable options: List name, description and navigation, Versioning settings, Advanced settings, Validation settings, Column default value settings, Audience targeting settings, Rating settings, and Form settings. Under Permissions and Management, there are options for Permissions for this document library, Manage files which have no checked in version, Workflow Settings, and Enterprise Metadata and Keywords Settings. There's also a link to RSS settings. A note states: 'A column stores information about each document in the document library. The following columns are currently available in this document library.' A table lists columns: Created (Date and Time, Required), Modified (Date and Time), Title (Single line of text), Description (Multiple lines of text), Created By (Person or Group), Modified By (Person or Group), and Checked Out To (Person or Group). At the bottom, there are links for Create column, Add from existing site columns, Column ordering, and Indexed columns.

I click the permissions to edit them

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint interface. At the top, there's a navigation bar with tabs like 'New tab', 'Active sites - SharePoint', and 'Permissions: Document'. Below the bar, the SharePoint logo is visible. A dropdown menu is open under the 'PERMISSIONS' tab, with the 'Stop Inheriting Permissions' option highlighted by a mouse cursor. A tooltip for this option states: 'Copy permissions from parent, and then stop inheriting permissions.' To the right of the tooltip, a table lists permission levels for different groups:

Type	Permission Levels
SharePoint Group	Edit
SharePoint Group	Full Control
SharePoint Group	Read

Below the table, there are sections for 'Notebook', 'Pages', 'Site contents', and 'Recycle Bin', each with checkboxes for 'HR Owners' and 'HR Visitors'. At the bottom left, there's an 'EDIT LINKS' button.

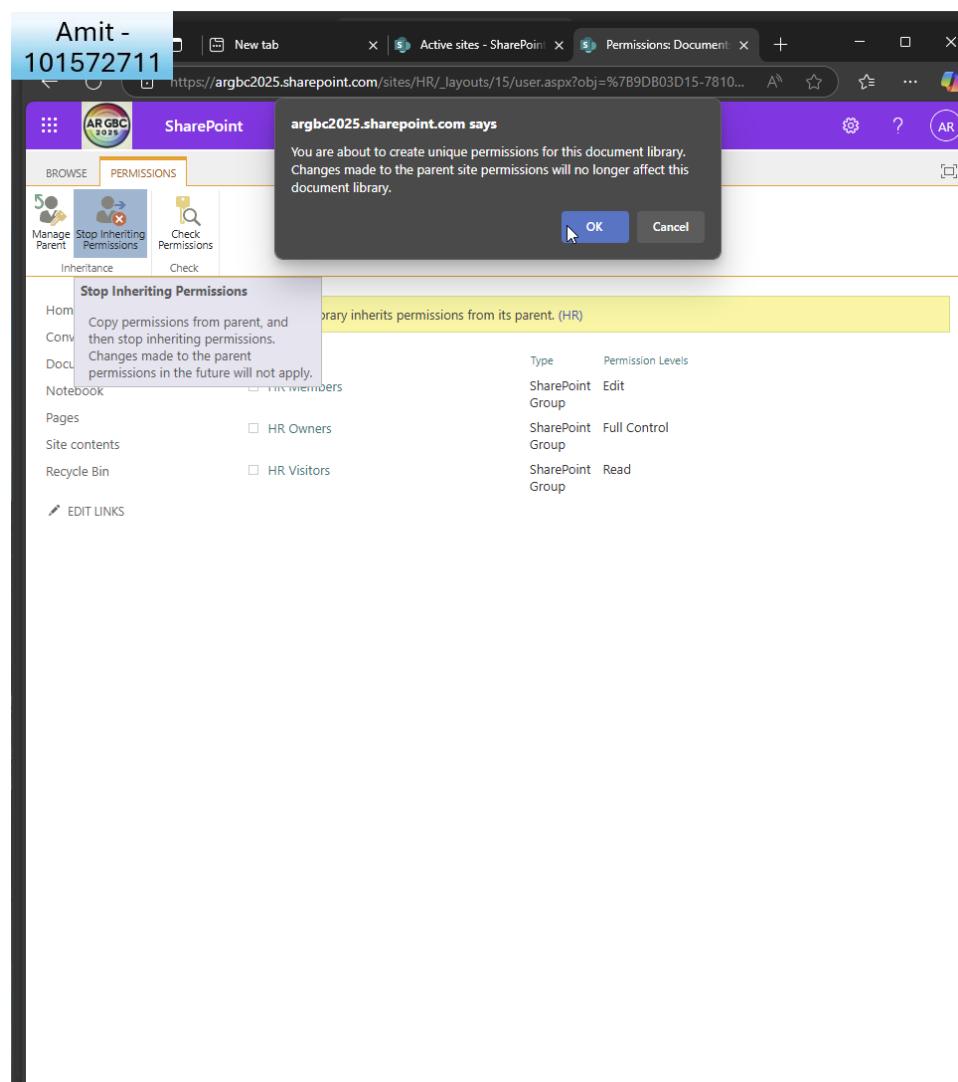
I click to stop inheriting permissions

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



It gives me a warning via a popup

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft SharePoint team site titled "IT". The top navigation bar includes "SharePoint", a search bar, and various site settings icons. On the left, there's a vertical navigation menu with options like "New", "Page details", and "Analytics". The main content area features a "News" section with a "Keep your team updated" card and an "Activity" section showing recent posts from the "IT" group. To the right, a "Next steps" sidebar provides links to "Apply a site template", "Invite team members", "Upload files", "Post news", and "Change the look".

I do the same for IT department.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Edge browser window with the title bar "Amit - 101572711" and the address bar "https://argbc2025.sharepoint.com/sites/IT/_layouts/15/user.aspx". The SharePoint ribbon has "SharePoint" selected. The "PERMISSIONS" tab is active. Below the tabs are four buttons: "Grant Permissions" (Grant), "Edit User Permissions" (Modify), "Check Permissions" (Check), and "Manage" (Manage). A "Permission Levels" section includes "Access Request Settings" and "Site Collection Administrators". The main content area displays a table of permissions:

	Name	Type	Permission Levels
Home	<input type="checkbox"/> <input checked="" type="checkbox"/> Name	SharePoint Group	Edit
Conversations	<input type="checkbox"/> <input checked="" type="checkbox"/> IT Members	SharePoint Group	Full Control
Documents	<input type="checkbox"/> <input checked="" type="checkbox"/> IT Owners	SharePoint Group	Read
Notebook	<input type="checkbox"/> <input checked="" type="checkbox"/> IT Visitors	SharePoint Group	
Pages			
Site contents			
Recycle Bin			

At the bottom left is a "EDIT LINKS" button.

I see the permissions

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint interface with a purple header bar. The title bar displays "Amit - 101572711" and the URL "https://argbc2025.sharepoint.com/sites/IT/_layouts/15/user.aspx?obj=%7B9DB03D15-7810-4C8E-BF0A-000000000000%7D". The main content area has a blue sidebar on the left with options like "Manage Parent", "Stop Inheriting Permissions", and "Check Permissions". The main pane shows a "Stop Inheriting Permissions" dialog box with the following text:
Home Copy permissions from parent, and
Copy permissions from parent, and then stop inheriting permissions.
Changes made to the parent
permissions in the future will not apply.
Notebook IT Members
Pages IT Owners
Site contents IT Visitors
Recycle Bin IT Visitors

On the right, there is a table of permission levels:

Type	Permission Levels
SharePoint Group	Edit
SharePoint Group	Full Control
SharePoint Group	Read

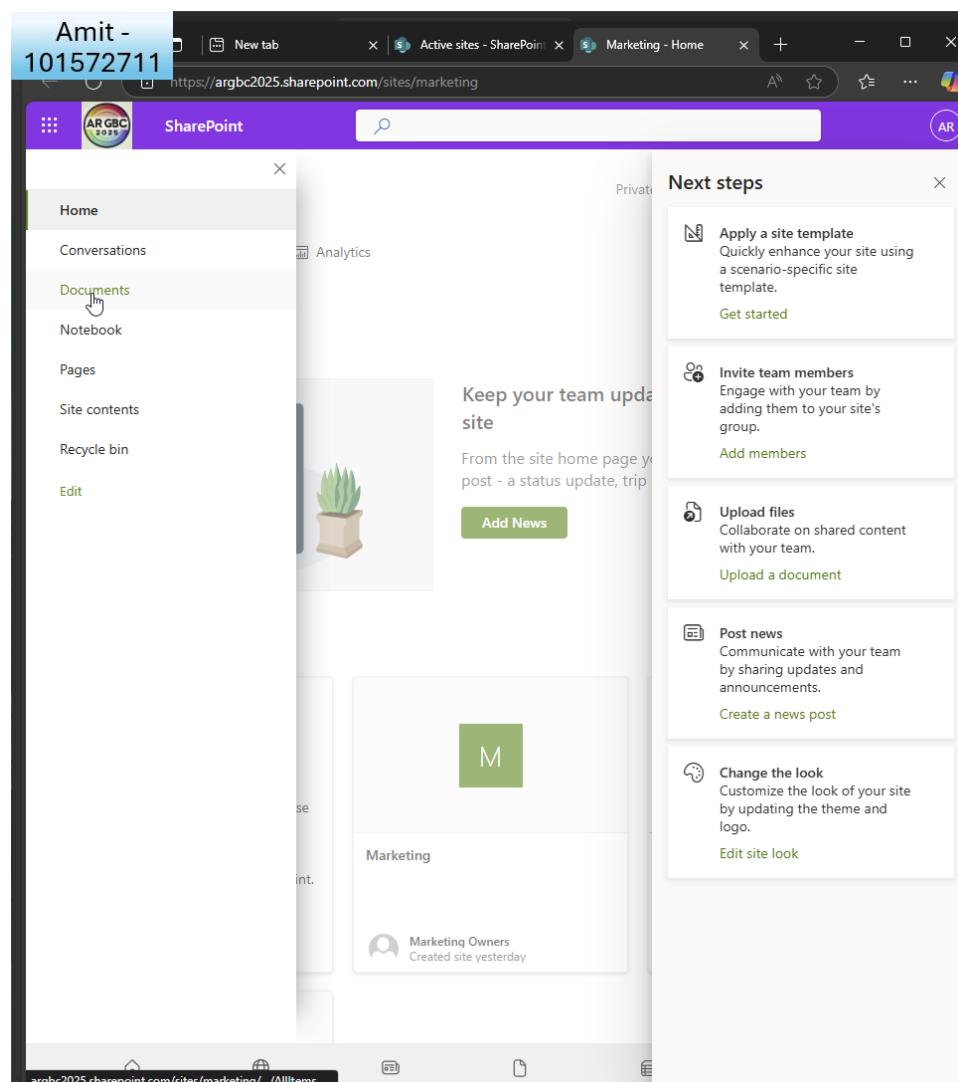
I click to stop inheriting permissions

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



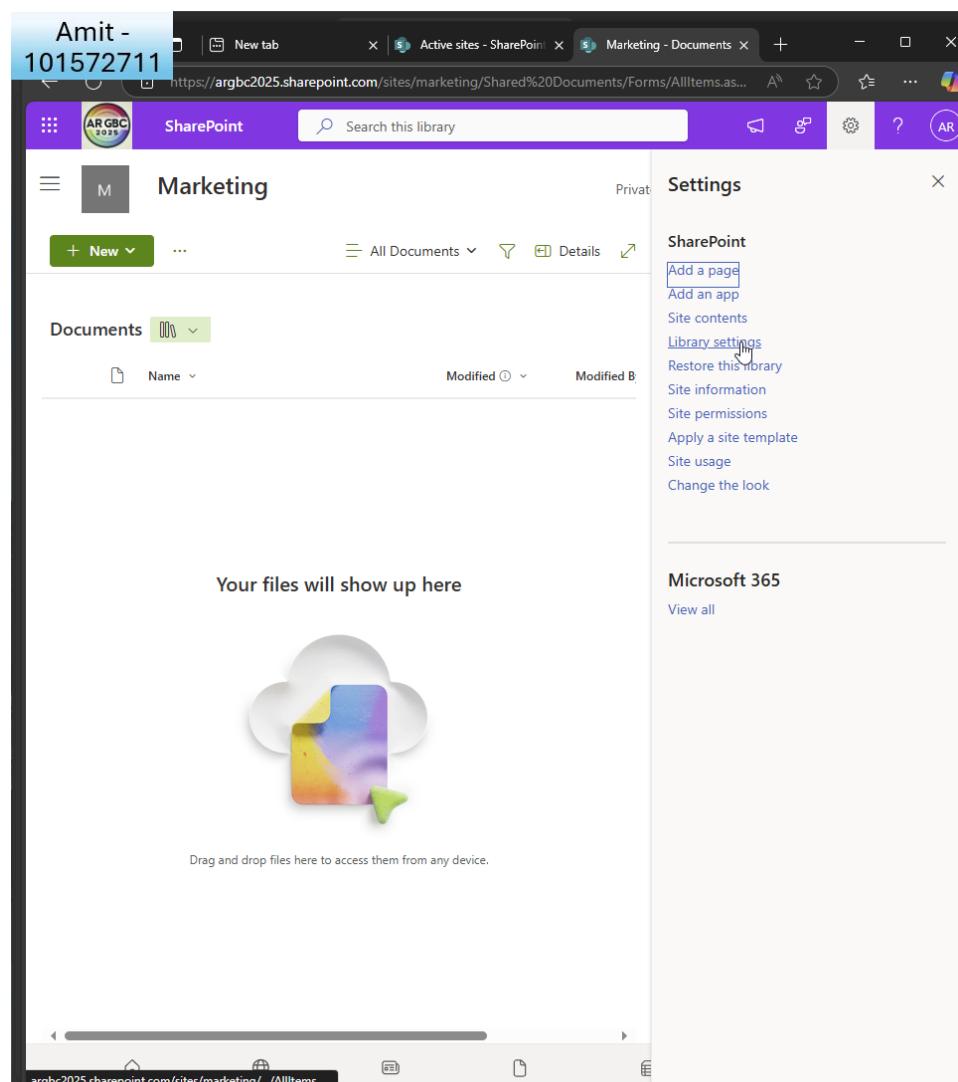
I do the same for the marketing site

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I click the library settings

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint interface. At the top, there's a navigation bar with tabs like 'New tab', 'Active sites - SharePoint', and 'Permissions: Document'. Below the bar, a purple header says 'SharePoint' with a 'PERMISSIONS' tab selected. On the left, there's a sidebar with icons for 'Manage Parent', 'Stop Inheriting Permissions' (which is highlighted), and 'Check Permissions'. The main content area has a title 'Stop Inheriting Permissions' with a tooltip explaining it: 'Copy permissions from parent, and then stop inheriting permissions.' It also says 'Changes made to the parent permissions in the future will not apply.' Below this, there's a table showing permission levels for different groups:

	Type	Permission Levels
Marketing Members	SharePoint Group	Edit
Marketing Owners	SharePoint Group	Full Control
Marketing Visitors	SharePoint Group	Read

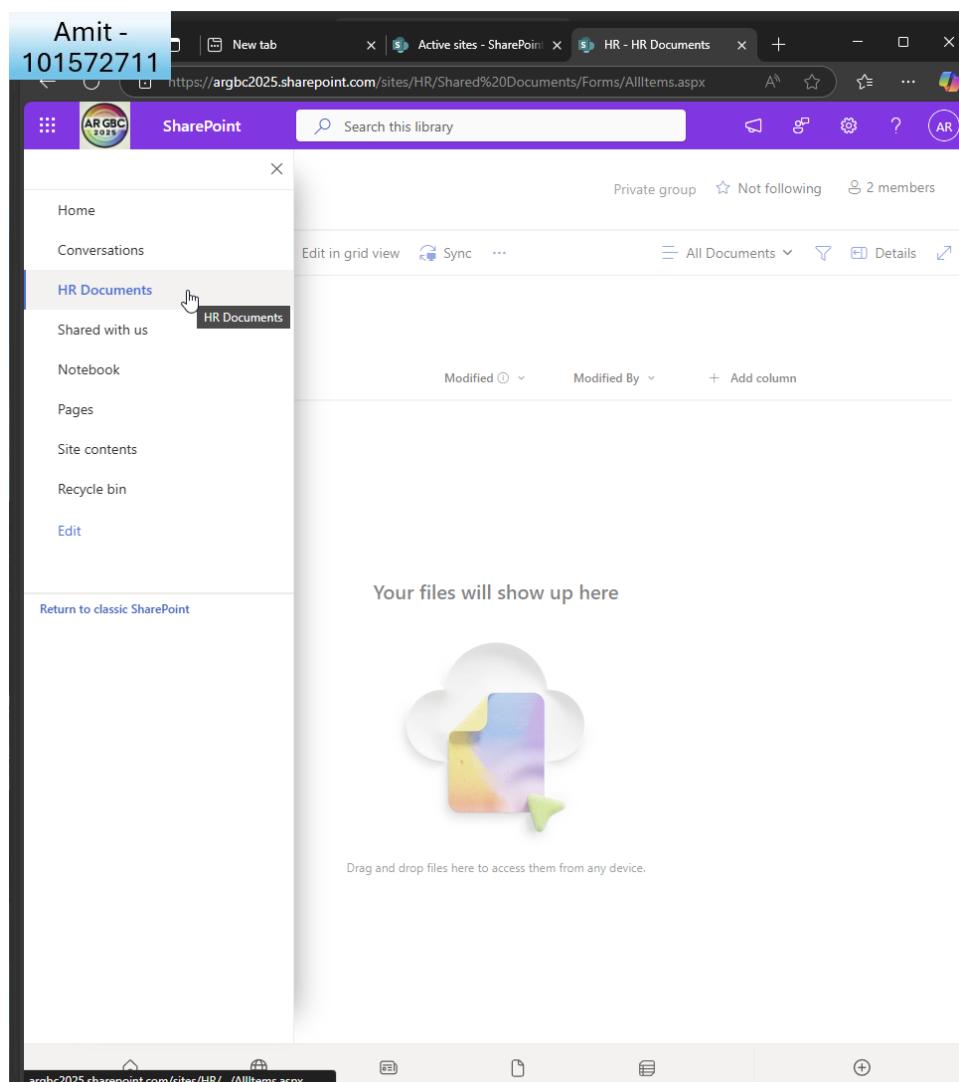
At the bottom left, there's a link 'EDIT LINKS'.

I stop inheriting permissions once more

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

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

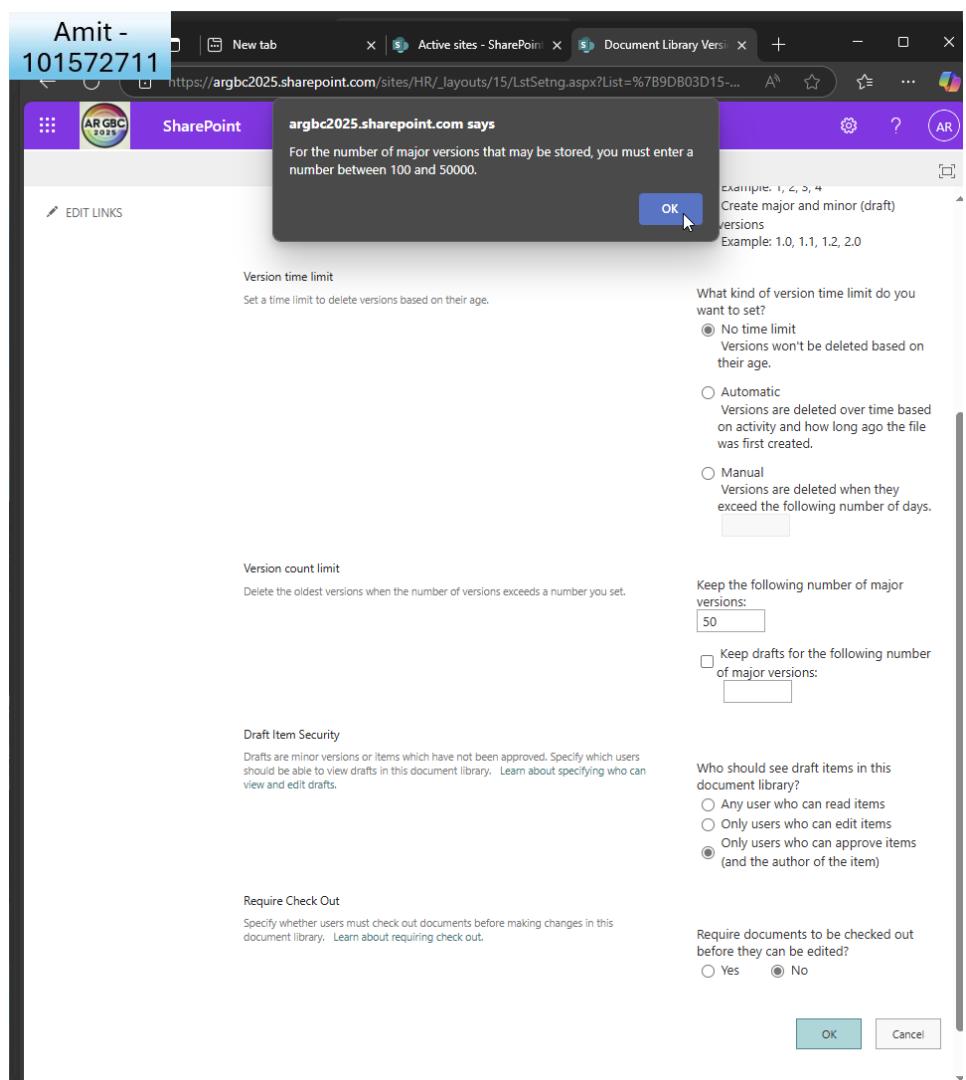
The screenshot shows the 'HR Documents' settings page in SharePoint. On the left, there's a navigation menu with links like Home, Conversations, HR Documents, Notebook, Pages, Site contents, Recycle Bin, and EDIT LINKS. The main content area has sections for List Information (Name: HR Documents, Web Address: https://argbc2025.sharepoint.com/sites/HR/Shared%20Documents/Forms/AllItems.aspx), General Settings, Permissions and Management, Communications, and Columns. Under General Settings, there's a list of settings including 'List name, description and navigation', 'Versioning settings' (which is highlighted with a red box and a cursor arrow), 'Advanced settings', 'Validation settings', 'Column default value settings', 'Audience targeting settings', 'Rating settings', and 'Form settings'. Below these, under 'Columns', it says 'A column stores information about each document in the document library. The following columns are currently available in this document library:' followed by a table with columns for 'Column (click to edit)', 'Type', and 'Required'. The columns listed are Created (Date and Time), Modified (Date and Time), Title (Single line of text), Description (Multiple lines of text), Created By (Person or Group), Modified By (Person or Group), and Checked Out To (Person or Group). At the bottom, there are links for 'Create column', 'Add from existing site columns', 'Column ordering', and 'Indexed columns'.

whilst in the document settings I click versioning settings

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Document Library Versioning' settings page in SharePoint. The URL is https://argbc2025.sharepoint.com/sites/HR/_layouts/15/LstSetng.aspx?List=%7B9D803D15-...'. The page has a purple header bar with the SharePoint logo and a circular icon for 'AR GBC 2025'. On the left, there's a navigation menu with links like Home, Conversations, HR Documents, Notebook, Pages, Site contents, and Recycle Bin. Below the menu is a 'EDIT LINKS' button. The main content area is divided into several sections:

- Content Approval:** A section about requiring approval for submitted items. It includes a radio button for 'Yes' (selected) and 'No'.

Require content approval for submitted items?
 Yes No
- Document Version History:** A section about creating versions each time a file is edited. It includes a radio button for 'Create major and minor (draft)' (selected) and 'Create major versions'.

Create a version each time you edit a file in this document library?
 Create major and minor (draft)
Example: 1.0, 1.1, 1.2, 2.0
 Create major versions
Example: 1, 2, 3, 4
- Version time limit:** A section for deleting old versions based on age. It includes a radio button for 'No time limit' (selected).

Set a time limit to delete versions based on their age.
 No time limit
Versions won't be deleted based on their age.
- Version count limit:** A section for deleting old versions when the number of versions exceeds a set limit. It includes a radio button for 'Automatic' (selected).

Delete the oldest versions when the number of versions exceeds a number you set.
 Automatic
Versions are deleted over time based on activity and how long ago the file was first created.
- Draft Item Security:** A section about who can view and edit draft items. It includes a radio button for 'Only users who can approve items (and the author of the item)' (selected).

Drafts are minor versions or items which have not been approved. Specify which users should be able to view drafts in this document library. Learn about specifying who can view and edit drafts.
 Only users who can approve items (and the author of the item)
- Keep the following number of major versions:** A text input field containing '100'.

Keep the following number of major versions:
- Keep drafts for the following number of major versions:** A text input field with a dropdown arrow. The visible part shows '100'.

Keep drafts for the following number of major versions:
- Who should see draft items in this document library?** A section with three radio buttons:
 - Any user who can read items
 - Only users who can edit items
 - Only users who can approve items (and the author of the item)

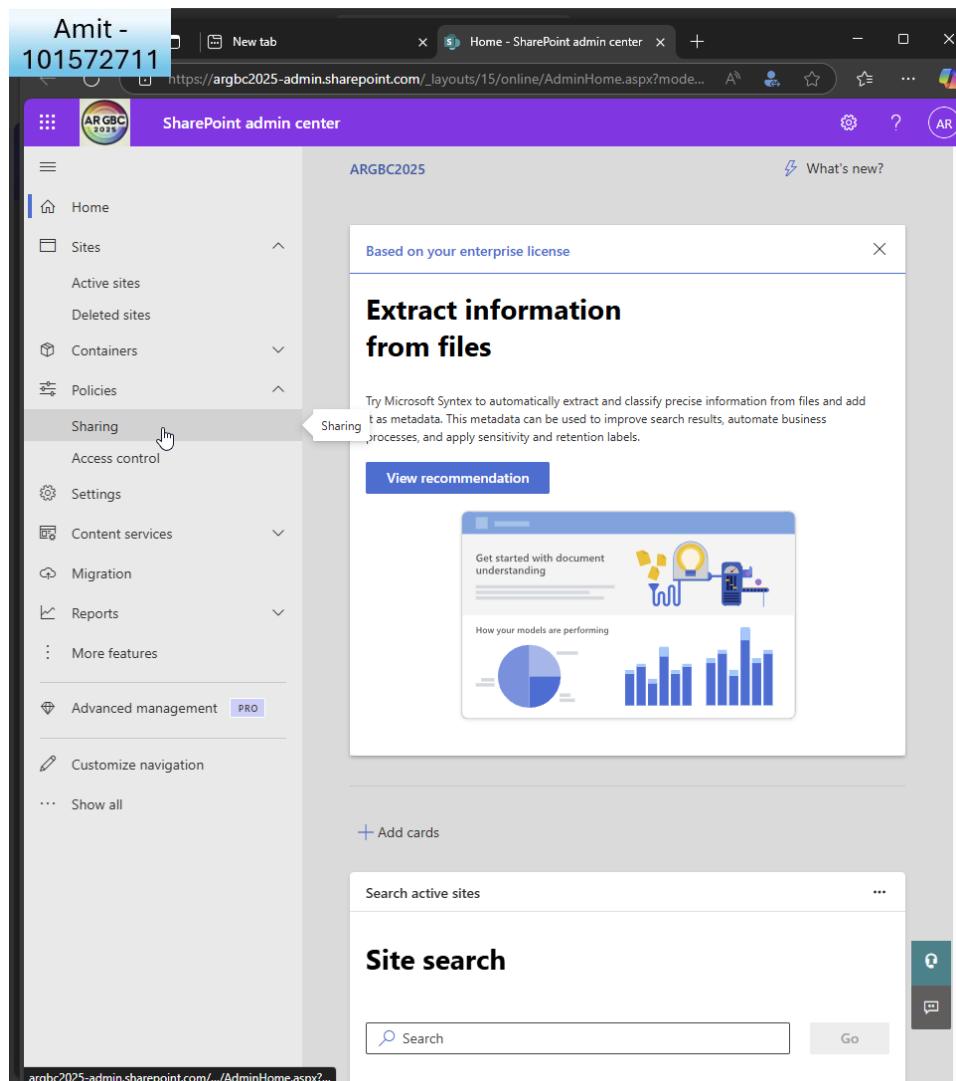
Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

2. Implement OneDrive for Business:

- Configure OneDrive settings to restrict external sharing.



I go to the sharepoint admin centre

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the SharePoint admin center interface with a purple header bar. The left sidebar menu includes Home, Sites, Active sites, Deleted sites, Containers, Policies (selected), Sharing (highlighted in blue), Access control, Settings, Content services, Migration, Reports, More features, Advanced management (PRO), Customize navigation, and Show all. The main content area is titled 'Sharing' and contains the following sections:

- External sharing**: A section titled "Content can be shared with:" with two tabs: "SharePoint" (selected) and "OneDrive". It features a vertical slider scale from "Most permissive" (top) to "Least permissive" (bottom). The "Least permissive" setting is currently selected, which corresponds to the "Only people in your organization" option. Other options include "Anyone", "New and existing guests", and "Existing guests".
- File and folder links**: A section where users can choose the type of link selected by default when sharing files and folders. The "Anyone with the link" option is selected. It also allows choosing the permission level for sharing links, with "View" selected.

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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. On the left is a vertical navigation bar with various icons. The main area is titled 'All admin centers' and contains a table with columns for 'Name' and 'Description'. The 'Microsoft Purview' row is highlighted with a gray background and a cursor is pointing at it. Other items in the list include Dynamics 365 Apps, Exchange, Microsoft Defender ATP, Microsoft Defender for Identity, Microsoft Entra, Microsoft Intune, Office configuration, Power Automate, Power BI, Power Platform, and Search & intelligence.

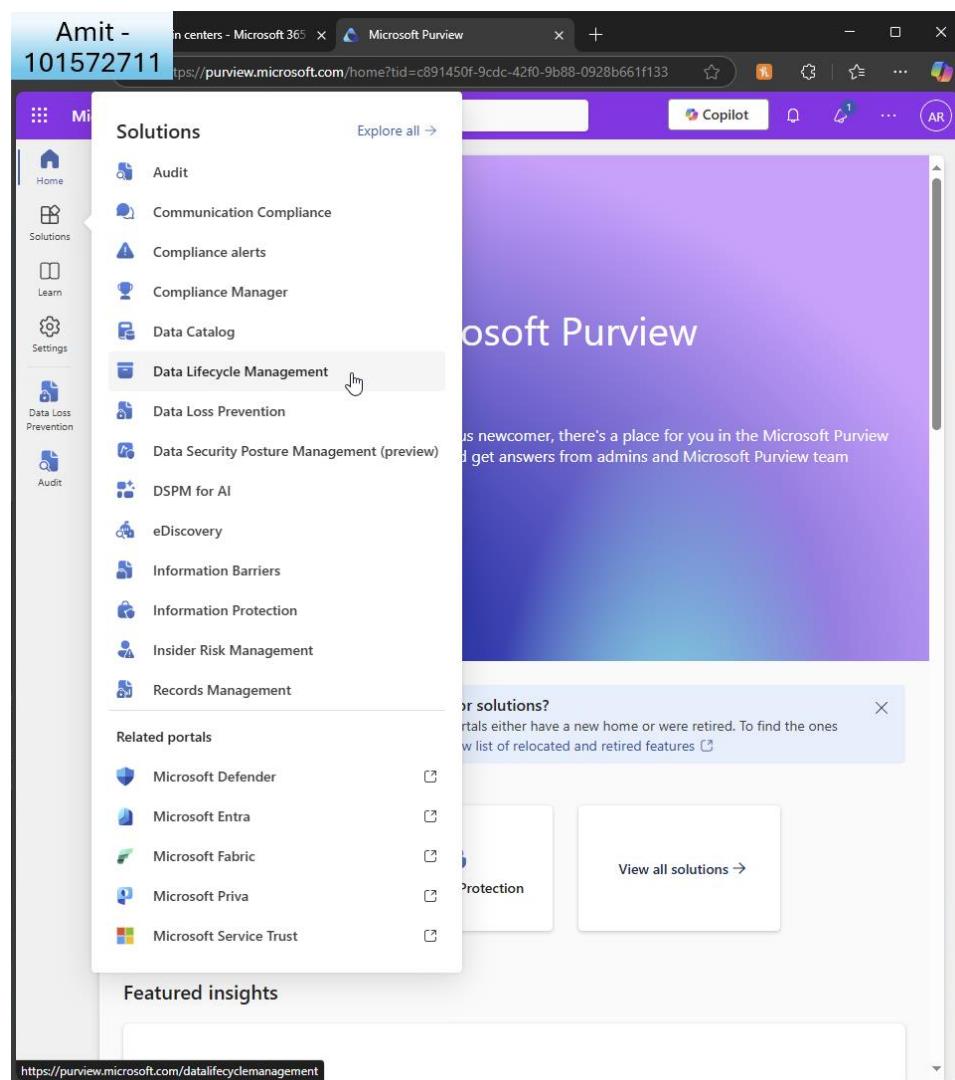
Name	Description
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.

I go to MS purview

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



I click to create a DLP policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview interface for Data Lifecycle Management. The left sidebar has a 'Policies' section expanded, with 'Retention policies' highlighted. The main content area is titled 'Overview' and discusses data lifecycle management tools for retaining content. It shows a section for 'Most used retention labels' with a message: 'No retention labels detected'. Below this are 'Data lifecycle management resources' and a 'Stay informed about data lifecycle management' section with links to official docs, news, videos, and Microsoft Purview updates.

I click 'retention policies'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview interface for Data Lifecycle Management. The left sidebar has a 'Policies' section expanded, with 'Retention policies' selected. The main area is titled 'Retention policies' and contains a note about role group permissions. It shows a table with one item: 'Email and Docs Retention – 2 Years' created by 'Amit Ratnapark'. A button '+ New retention policy' is visible.

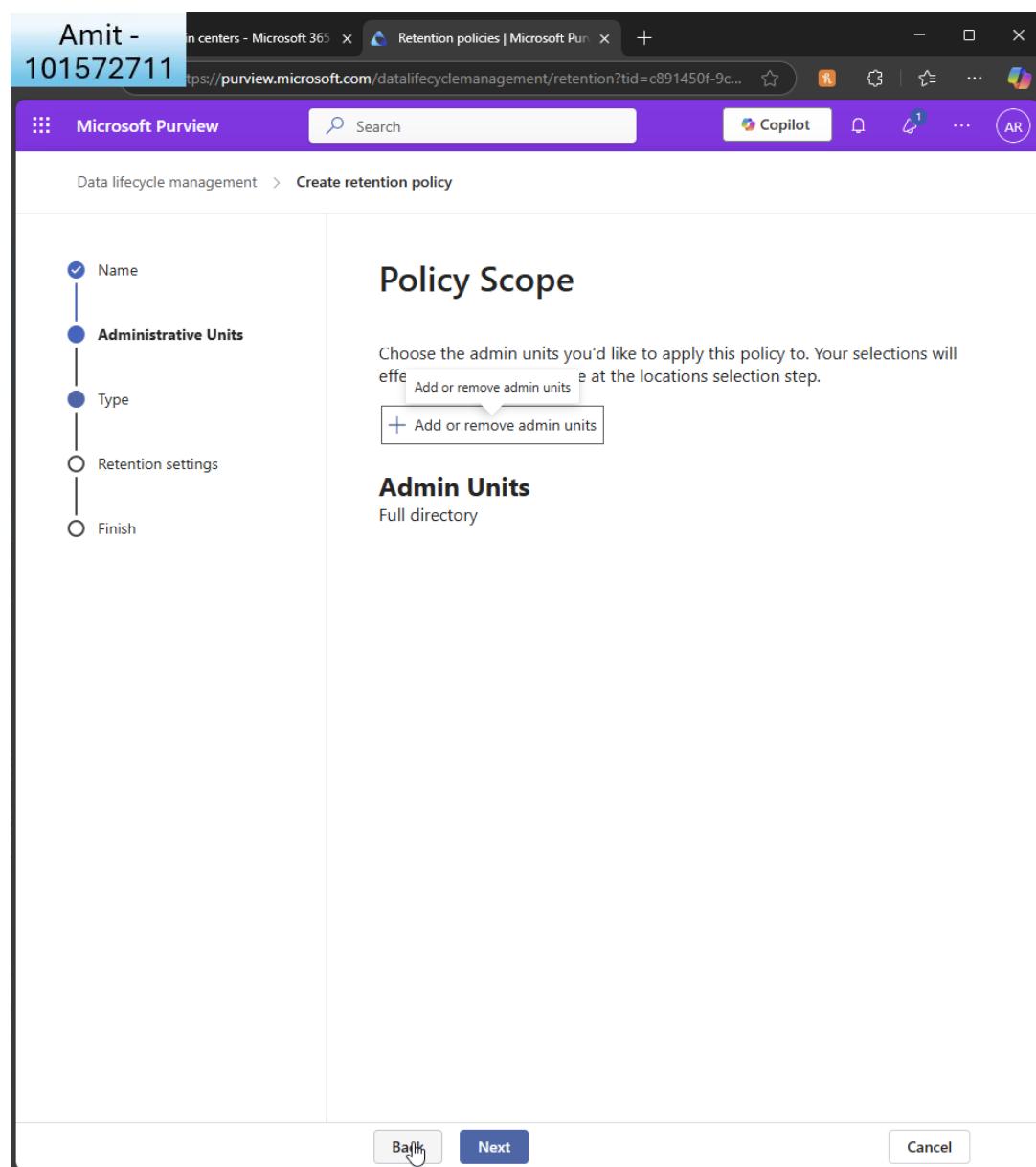
https://purview.microsoft.com/datalifecyclemanagement/retention?tid=c891450f-9cdc-42f0-9b88-0928b661f133

And create a new retention policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

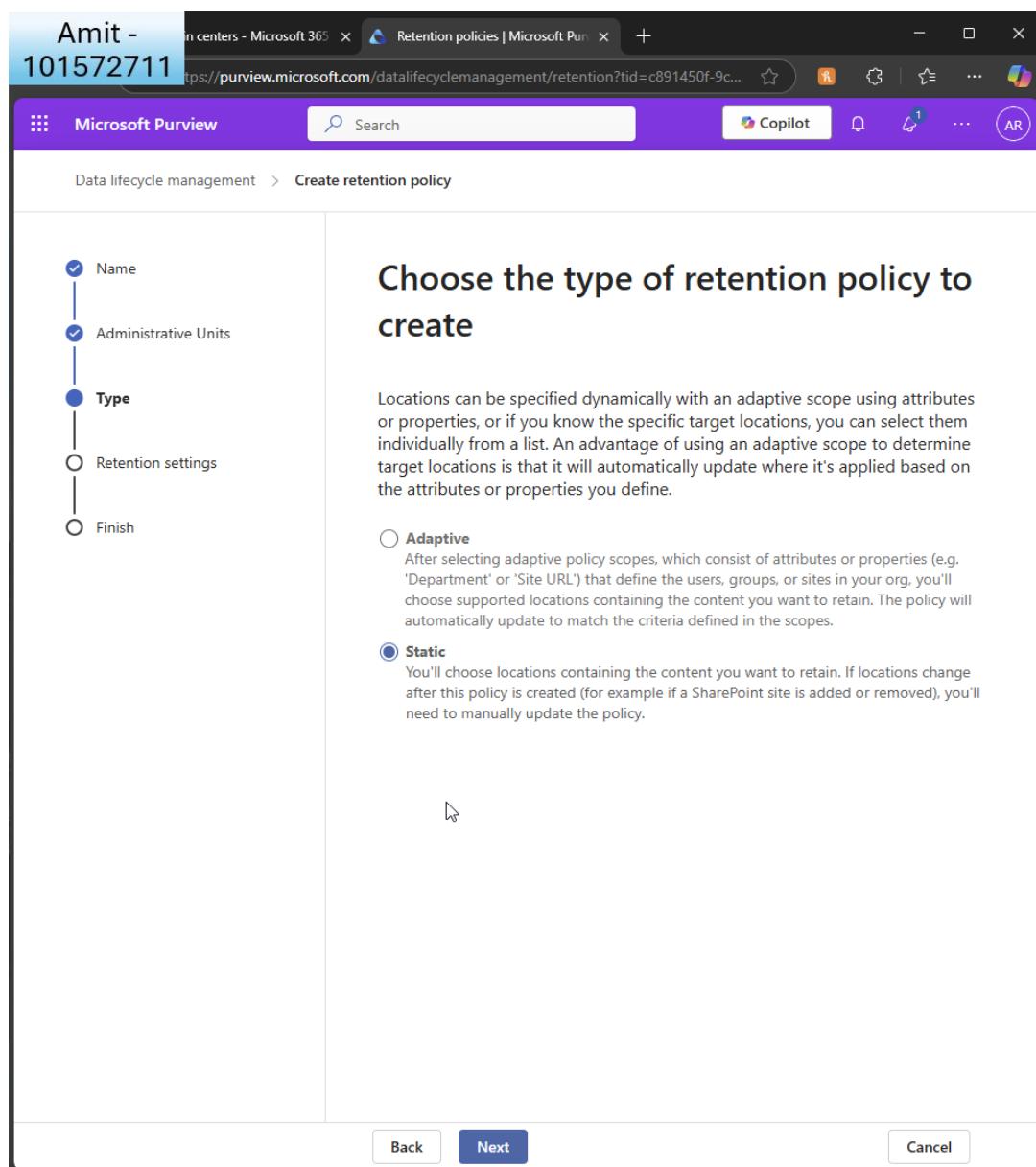


I leave it for all admin units

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



I choose 'static'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create retention policy' wizard in Microsoft Purview. The left sidebar lists steps: Name (checkmark), Administrative Units, Type (selected), Locations, Retention settings, and Finish. The main area title is 'Choose where to apply this policy'. It says 'The policy will apply to content that's stored in the locations you choose.' A note indicates you can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp, and many more. The 'Type' section contains several location options with status switches:

Status	Location	Applicable Content
Off	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, and tasks with an end date. Doesn't apply to items in Microsoft 365 Group mailboxes. More details
Off	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details
On	OneDrive accounts	All files in users' OneDrive accounts. More details
Off	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. More details
Off	Skype for Business	Skype conversations for the users you choose.
Off	Exchange public folders	Items from all Exchange public folders in your organization
Off	Teams channel	Messages from channel conversations and channel

At the bottom are 'Back', 'Next', and 'Cancel' buttons.

I apply it only to onedrive accounts

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview Data Lifecycle Management interface for creating a retention policy. The title bar indicates the user is 'Amit - 101572711'. The main heading is 'Create retention policy'. On the left, a vertical navigation pane lists steps: 'Name' (checked), 'Administrative Units' (checked), 'Type' (checked), 'Retention settings' (selected), and 'Finish' (unchecked). The right panel contains the configuration for 'Retention settings'. It features a title 'Decide if you want to retain content, delete it, or both' and a summary: 'Items will be retained for the period you choose.' Below this, under 'Retain items for a specific period', a dropdown menu shows '5 years'. Under 'Start the retention period based on', a dropdown menu shows 'When items were created'. Under 'At the end of the retention period', two options are shown: 'Delete items automatically' (selected) and 'Do nothing'. Other options include 'Retain items forever' and 'Only delete items when they reach a certain age'. At the bottom of the panel are 'Back', 'Next', and 'Cancel' buttons.

I choose to retain for 5 years and delete items automatically

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser window titled 'Amit - 101572711'. The URL is <https://purview.microsoft.com/datalifecyclemanagement/retention?tid=c891450f-9c...>. The page is titled 'Create retention policy' under 'Data lifecycle management'. On the left, a vertical checklist shows steps completed (Name, Administrative Units, Type, Retention settings) and one step pending (Finish). The main right panel is titled 'Review and finish' and contains the following details:

- Policy name:** OneDrive 5-Year Retention ([Edit](#))
- Description:** ([Edit](#))
- Locations to apply the policy:** OneDrive accounts (All Sites) ([Edit](#))
- Retention settings:**
 - Retain items for 5 years based on when they were created
 - Delete items at end of retention period

[Edit](#)

A warning message in a callout box states: "⚠ Items that are currently older than 5 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted."

At the bottom are buttons for [Back](#), [Submit](#), and [Cancel](#).

I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview interface for creating a retention policy. On the left, a vertical checklist indicates the steps completed: Name, Administrative Units, Type, Retention settings, and Finish. The main area displays a success message: "You successfully created a retention policy". Below this, it says "Allow up to a week for the retention policy to be enforced". A section titled "Related tasks" includes links to "Create another retention policy", "Create an adaptive scope", and "Create a retention label", each with a "Get started" button. At the bottom, there is a "Recommendation" section with the text: "Save time and increase reliability of your policies by using adaptive scopes." It explains that adaptive scopes maintain policies automatically as things change in the organization. A "View Recommendation" button is available, and at the very bottom is a "Done" button.

It confirms it has been created

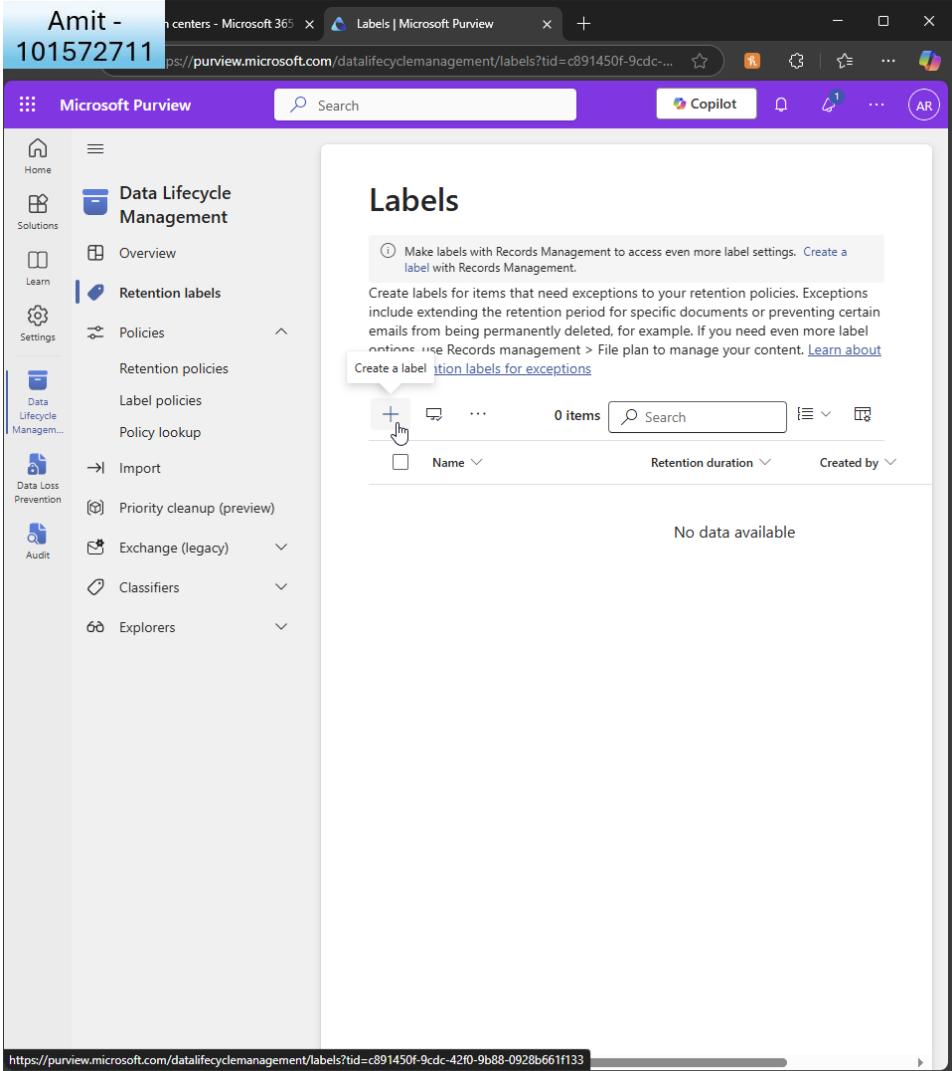
- Set up a policy to automatically move old files to the Recycle Bin after a year.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



The screenshot shows the Microsoft Purview interface for Data Lifecycle Management. The left sidebar has a 'Data Lifecycle Management' section expanded, showing 'Retention labels' selected. The main area is titled 'Labels' and contains a message about creating labels with Records Management. It includes a 'Create a label' button and a 'Priority cleanup (preview)' link. Below this is a table header with columns for 'Name', 'Retention duration', and 'Created by'. A message at the bottom states 'No data available'.

Still within DLP, I choose 'retention labels'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Labels interface titled "Create retention label". On the left, a vertical navigation bar lists steps: "Name" (selected), "Label Settings", "Period", and "Finish". The main area is titled "Name your retention label". It includes a note about Records Management, a "Name *" input field containing "1 Year Auto-Delete", and sections for "Description for users" and "Description for admins", both with placeholder text. At the bottom are "Next" and "Cancel" buttons.

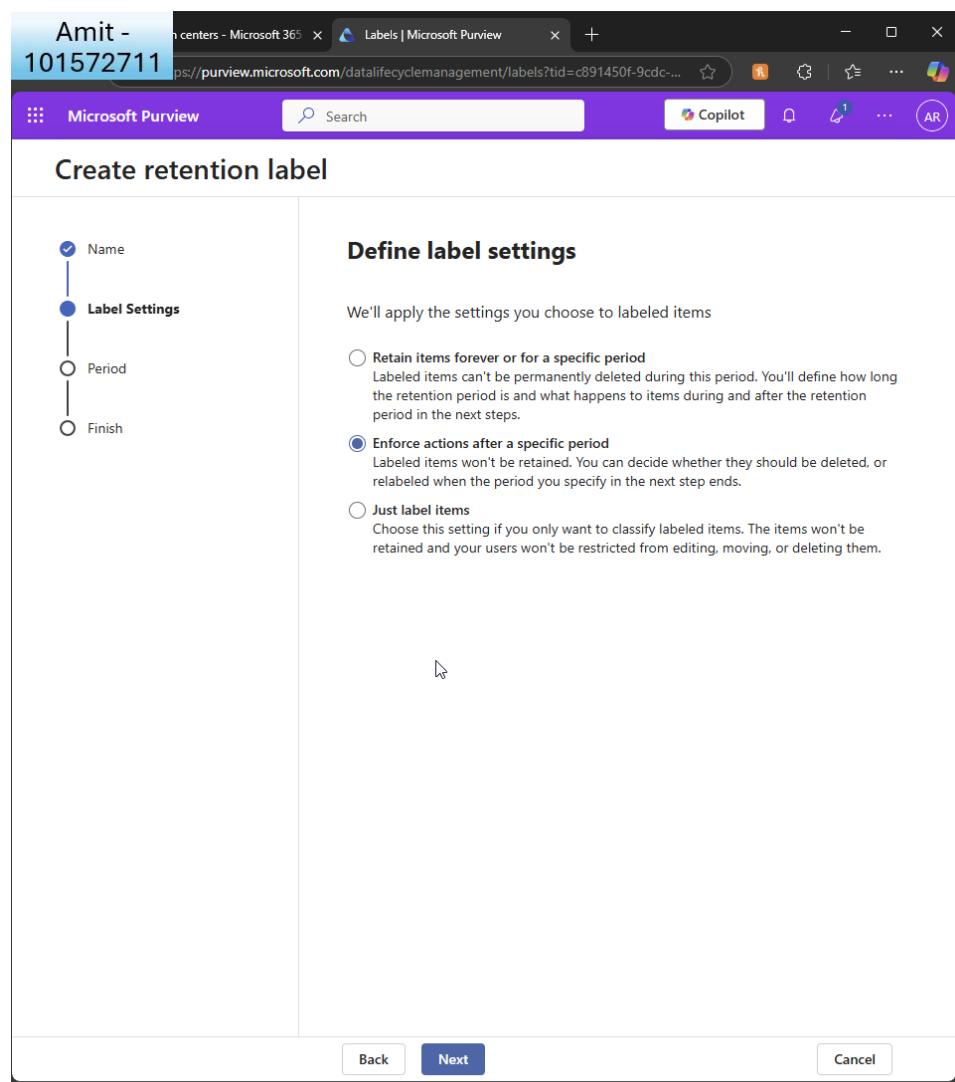
I name the retention label

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



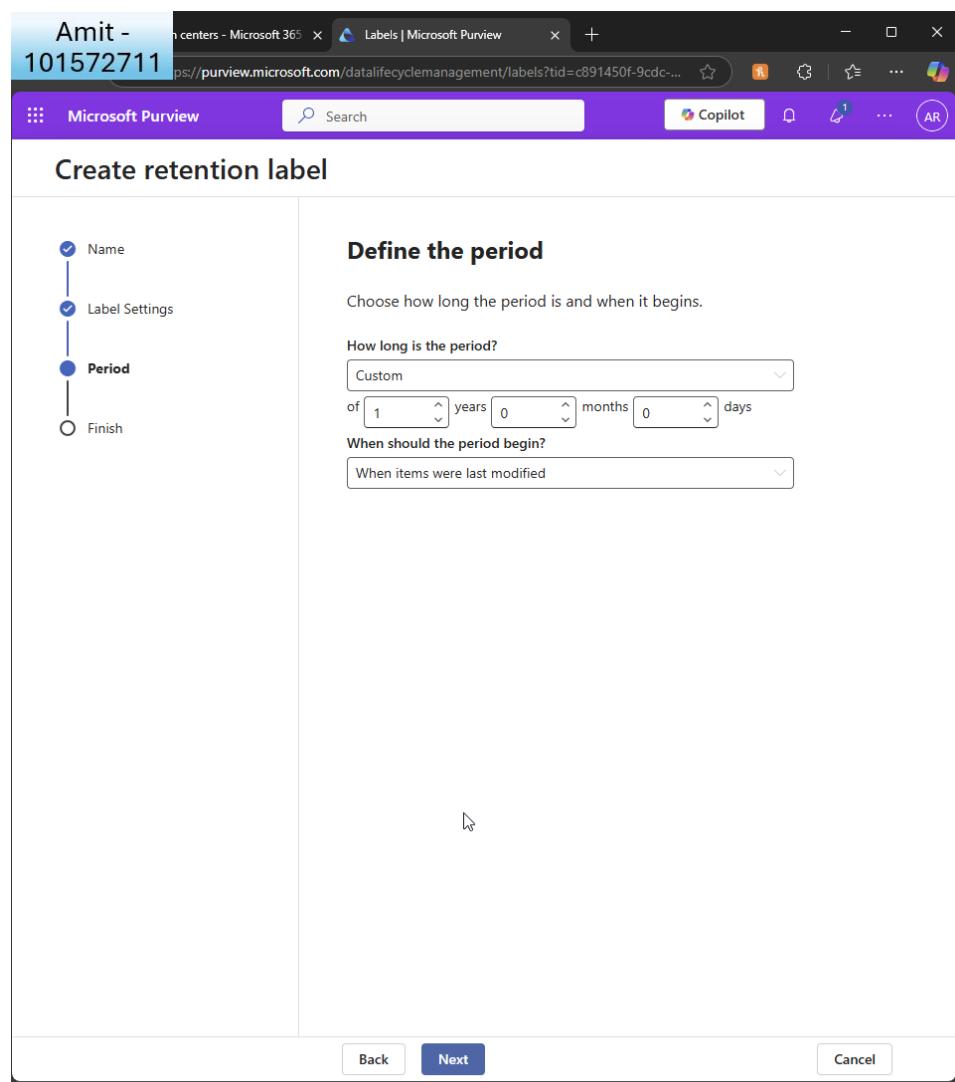
I enforce action after specific period i.e. 1 year

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



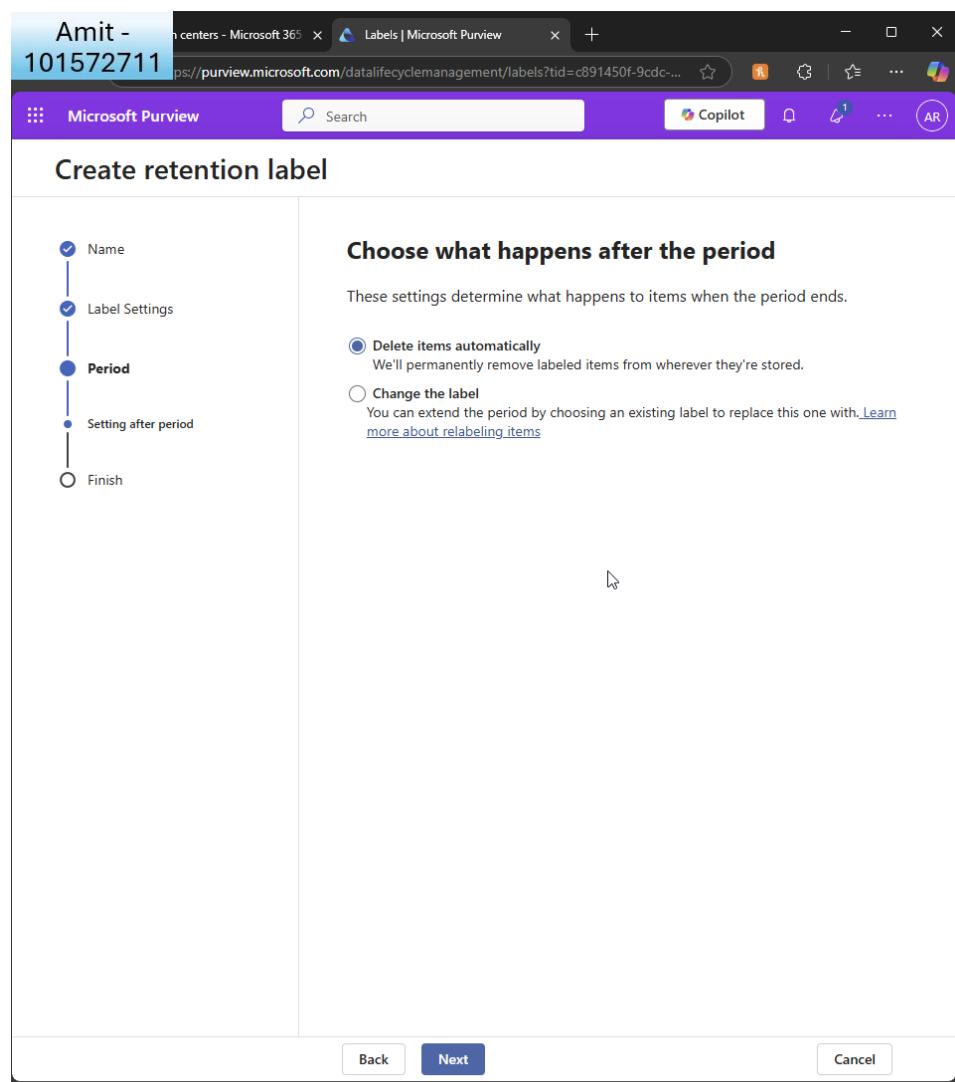
Here I specify 1 year retention from when the item was last modified.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



Here I choose the action to delete the items automatically

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Labels interface. At the top, it displays "Amit - 101572711" and the URL "https://purview.microsoft.com/datalifecyclemanagement/labels?tid=c891450f-9cdc-4...". The main area is titled "Create retention label". On the left, a vertical progress bar shows steps: "Name" (checkmark), "Label Settings" (checkmark), "Period" (checkmark), and "Finish" (blue dot). To the right, the "Review and finish" section is divided into two columns:

Name	Retention settings
Name 1 Year Auto-Delete Edit	Retention period 1 year Edit
Based on Based on when it was last modified Edit	Retention action Delete only Edit

At the bottom of the screen are buttons: "Back", "Create label" (highlighted in blue), and "Cancel".

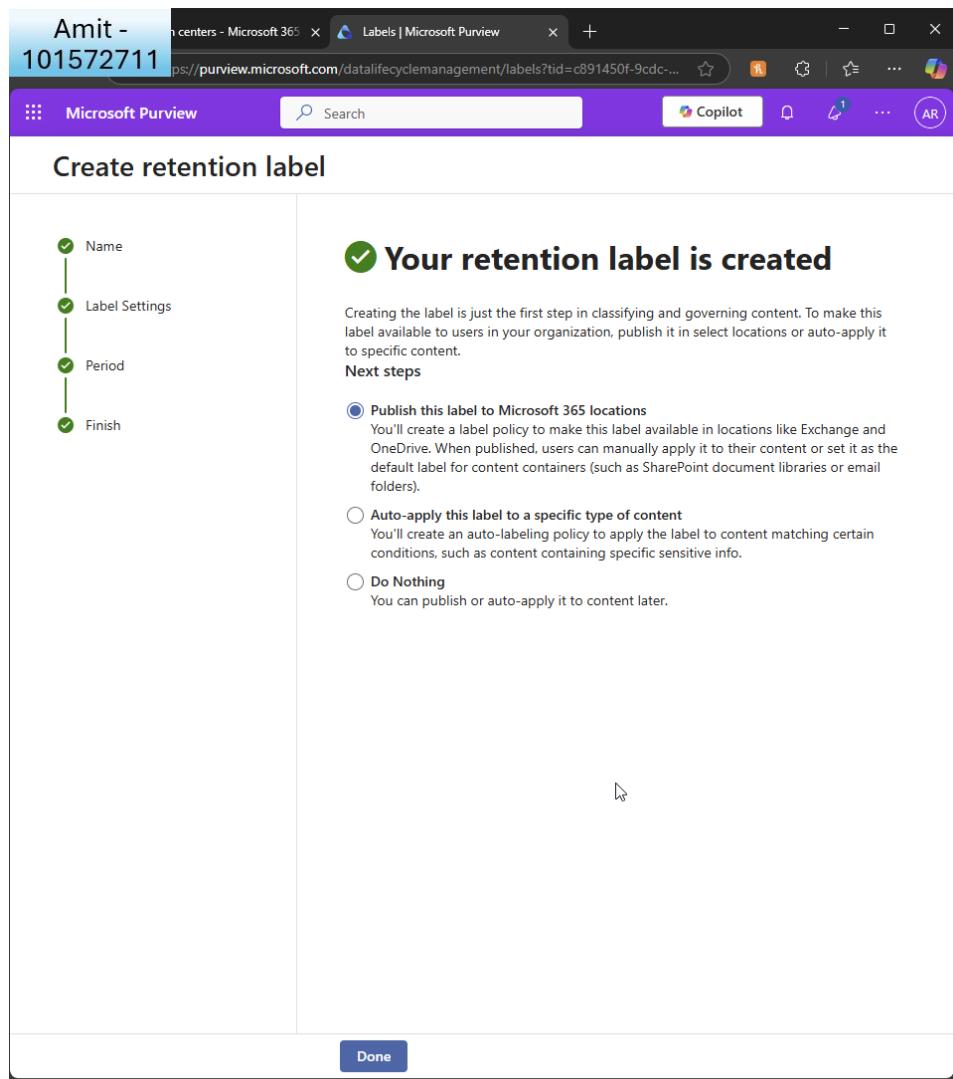
I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Labels interface. At the top, it displays the user's name and ID: "Amit - 101572711". The title bar says "Labels | Microsoft Purview". The main heading is "Publish labels so users can apply them to their content." On the left, a vertical navigation pane lists steps: "Choose labels to publish" (selected), "Administrative Units", "Scope", "Name your policy", and "Finish". The right pane is titled "Choose labels to publish" and contains instructions: "Choose the labels you want to publish to your organization's apps so users can apply them to their content. If you don't see the labels you want, you'll be able to create one from scratch." Below this, it says "Publish these labels (1 label(s))" and shows a table with one item:

Name	Retention
1 Year Auto-Del...	1 year delete

At the bottom, there are "Edit" and "Next" buttons.

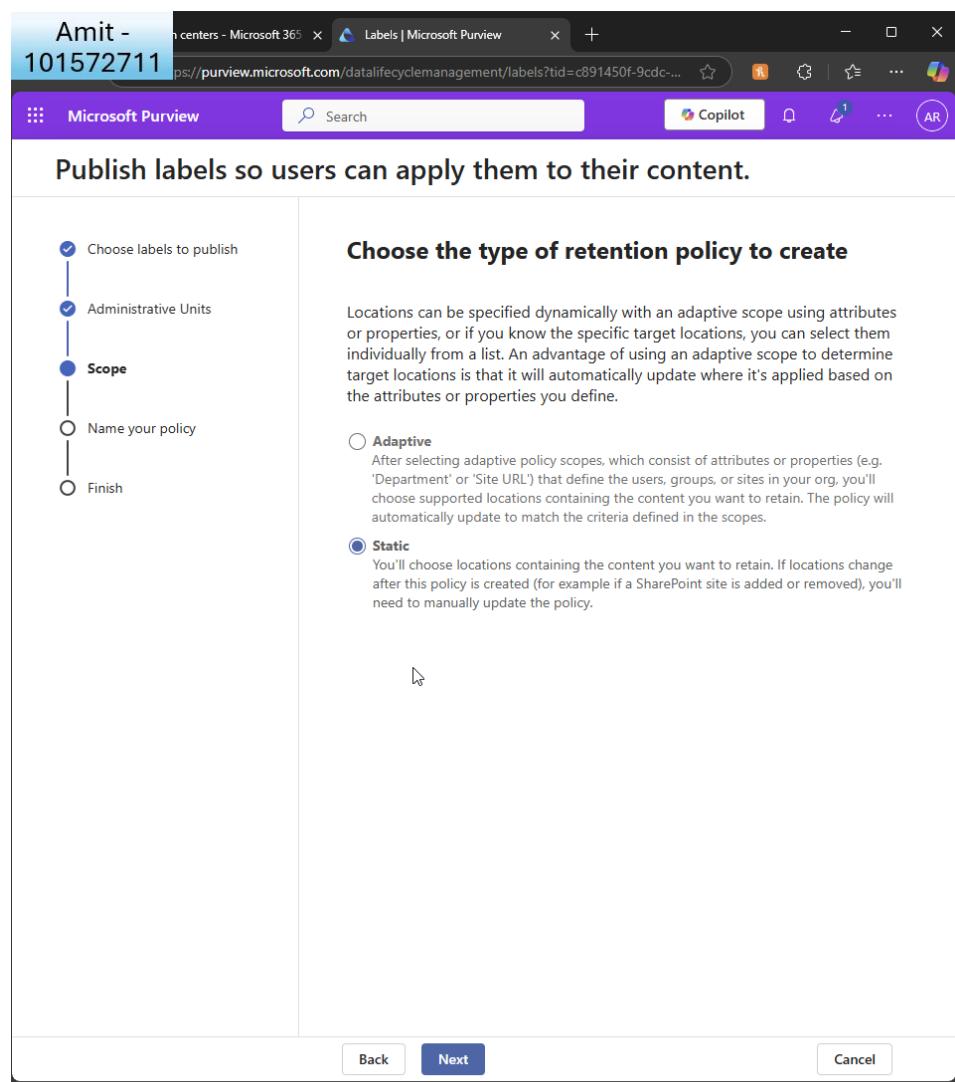
I now publish the label

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I choose 'static'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview browser window titled "Amit - 101572711". The URL is <https://purview.microsoft.com/datalifecyclemanagement/labels?tid=c891450f-9cdc-41d0-8a2e-1a2a2a2a2a2a>. The page displays a flow titled "Publish labels so users can apply them to their content." on the left, with a vertical list of steps: "Choose labels to publish" (checked), "Administrative Units" (checked), "Scope" (selected), "Publish to users and groups", "Name your policy", and "Finish". On the right, under "Choose where to publish labels", it says "When published, users in your organization will be able to apply this label to items in the locations you choose." There is a note about setting up data connectors. Below are four location options: "Exchange mailboxes" (Off), "SharePoint classic and communication sites" (Off), "OneDrive accounts" (On, All user accounts, Edit), and "Microsoft 365 Group mailboxes & sites" (Off). At the bottom are "Back", "Next", and "Cancel" buttons.

And specify only onedrive accounts

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Data Lifecycle Management Labels wizard window. The title bar reads "Amit - 101572711" and "Labels | Microsoft Purview". The main heading is "Publish labels so users can apply them to their content." On the left, a vertical navigation pane lists steps: "Choose labels to publish" (checkmark), "Administrative Units" (checkmark), "Scope" (checkmark), "Name your policy" (blue circle, currently selected), and "Finish" (empty circle). The right panel is titled "Name your policy". It contains a "Name *" field with the value "OneDrive Auto-Delete After 1 Year" and a "Description" field with the placeholder "Clearly describe this policy to users". At the bottom are "Back", "Next", and "Cancel" buttons.

I name the policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser window titled "Amit - 101572711". The URL is <https://purview.microsoft.com/datalifecyclemanagement/labels?tid=c891450f-9cdc-4...>. The page header includes "Microsoft Purview", a search bar, and various icons for Copilot, notifications, and AR.

The main content area has a title "Publish labels so users can apply them to their content." Below it, a vertical checklist on the left lists five steps: "Choose labels to publish" (checked), "Administrative Units" (checked), "Scope" (checked), "Name your policy" (checked), and "Finish" (unchecked). To the right of the checklist is a "Finish" section containing the following information:

- A warning message: **⚠ Most labels will become available to your users within a week. Labels will appear in Outlook and Outlook on the web only for mailboxes that have at least 10 MB of data.**
- "Choose labels to publish": 1 label(s) will be published (made available) so your users can classify their content
1 Year Auto-Delete 1 year delete
[Edit](#)
- "Applies to content in these locations": OneDrive accounts (All Sites)
[Edit](#)
- "Name": OneDrive Auto-Delete After 1 Year
[Edit](#)
- "Description":
[Edit](#)

At the bottom of the page are buttons for "Back", "Submit", and "Cancel".

I finish creating the policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview browser window with the URL [https://purview.microsoft.com/datalifecyclemanagement/labels?tid=c891450f-9cdc...](https://purview.microsoft.com/datalifecyclemanagement/labels?tid=c891450f-9cdc-4...). The title bar displays "Amit - 101572711". The main content area has a purple header "Microsoft Purview" and a search bar. A large green checkmark icon is prominently displayed next to the text "Your retention label was published". To the left, a vertical checklist shows five steps: "Choose labels to publish" (checkmark), "Administrative Units" (checkmark), "Scope" (checkmark), "Name your policy" (checkmark), and "Finish" (checkmark). Below the main message, there's a section titled "Related tasks" with three items: "Publish another retention label" (Get started button), "Auto-apply a retention label" (Get started button), and "Create a retention label" (Get started button). Further down, there's a "Set up default policies in MIP" section with a "Get started" button. At the bottom, a "Recommendation" box contains the text "Save time and increase reliability of your policies by using adaptive scopes." A "Done" button is at the very bottom.

I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

3. Set Up Viva Engage for Enterprise Social Networking:

- Configure Viva to allow only internal communications.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar contains various administrative icons. The main area lists several services with their descriptions. At the bottom of the list, the 'Viva Engage' option is highlighted with a mouse cursor. The URL <https://www.yammer.com/office365/admin> is visible at the bottom right of the list.

Icon	Service	Description
Dynamics 365 Apps	Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Search & intelligence	Manage Microsoft 365 Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.
Security	Security	Use Microsoft 365 Defender for unmatched visibility into threats to your network and your security posture. Respond to incidents, proactively hunt for threats, track your assets, and deploy policies to secure your identities, devices, Office 365 workspaces, apps, and more.
SharePoint	SharePoint	Manage sites, sharing, storage, and more for SharePoint and OneDrive. Migrate files and sites to Microsoft 365.
Universal Print	Universal Print	Universal Print is a serverless print management solution built with Zero Trust security in mind. Employees can print driverless from Windows 10/11, or Microsoft 365 for the web on mobile devices.
Viva Engage	Viva Engage	Manage your Yammer network, set a usage policy, control external network settings, and enable features like translation.

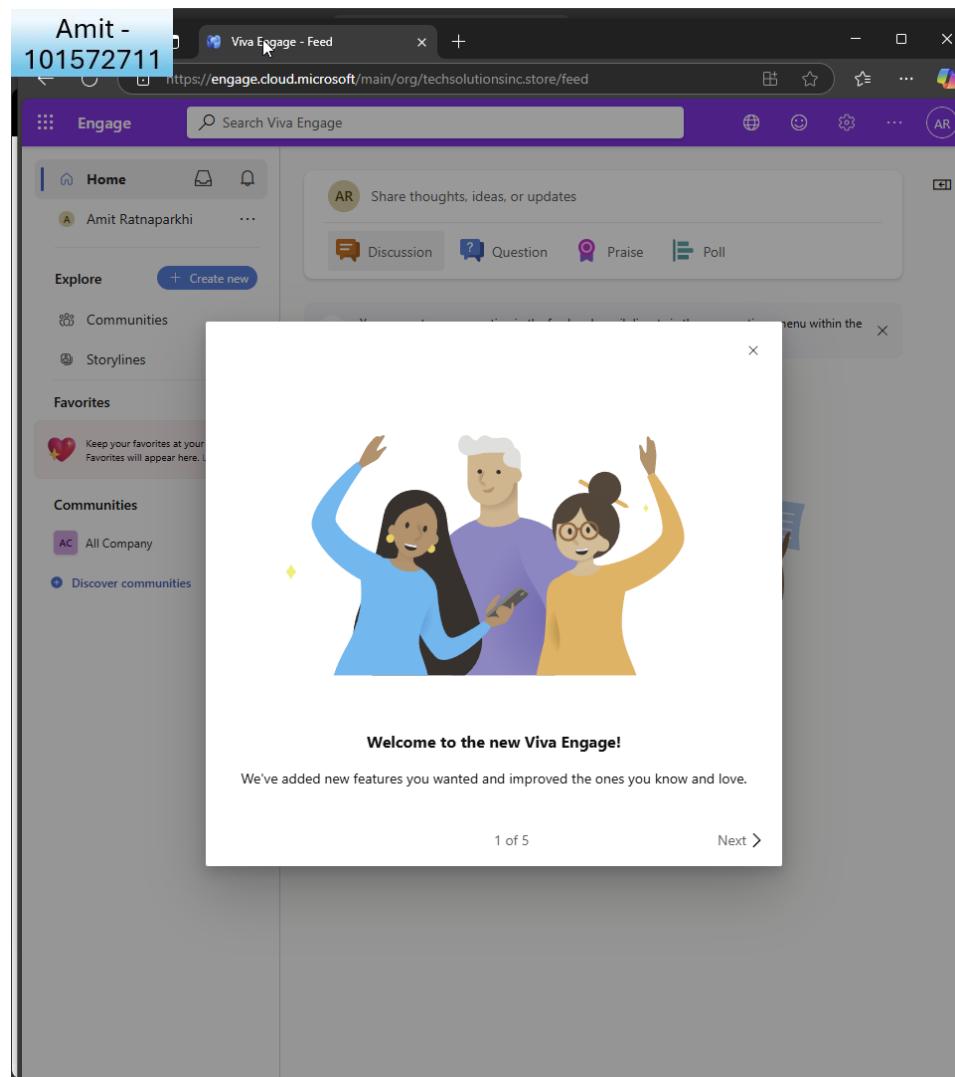
I choose 'Viva Engage' from all admin centres

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



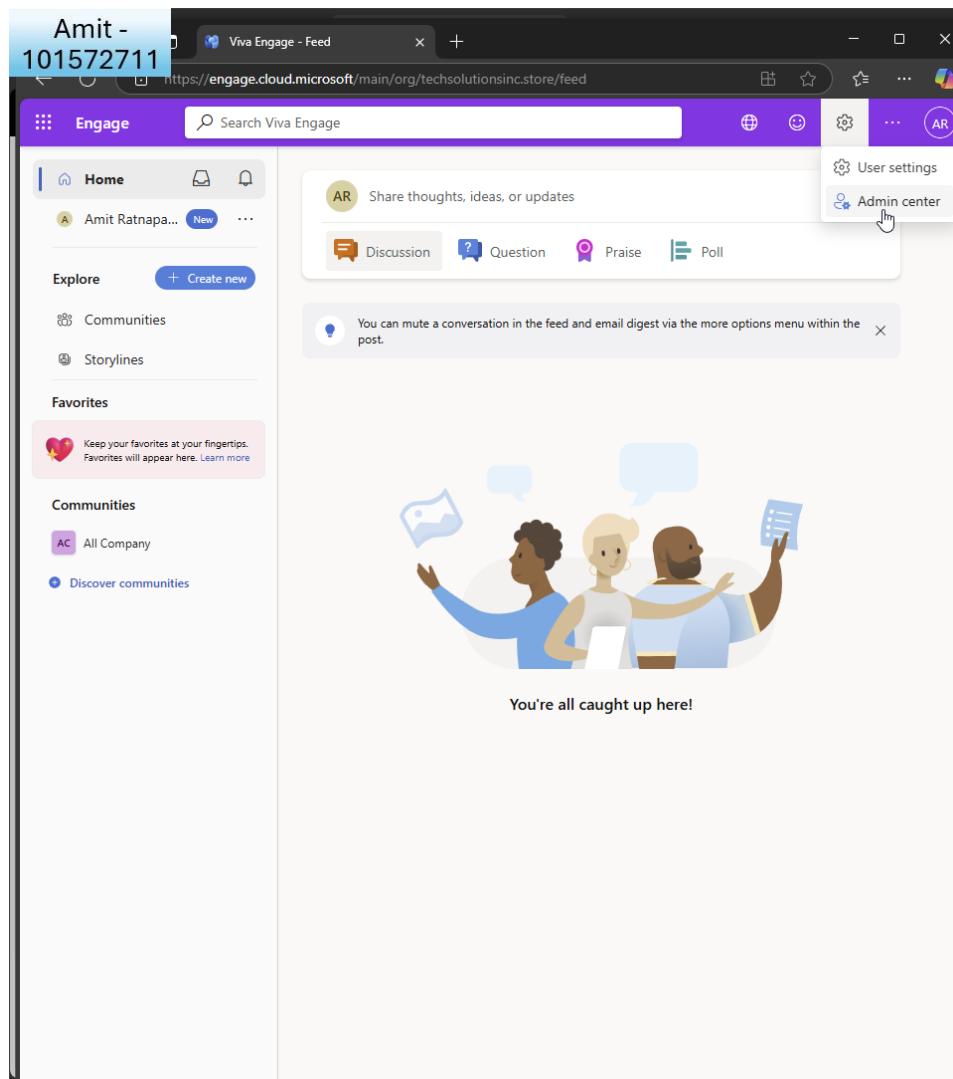
I see the welcome screen for the new viva engage

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I click 'admin cerntre'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Viva Engage tenant settings interface. At the top left, it displays "Amit - 101572711". The browser address bar shows the URL: <https://engage.cloud.microsoft/main/org/techsolutionsinc.store/admin/tenant-settings>. The main content area is titled "Tenant settings" with a "Learn more" link. It includes sections for "Viva Engage tenant name" (set to ARGBC2025), "Usage policy" (with an "Add" button), "Require users to review policy upon initial login and after updates" (switched off), "Tenant logo" (with an "Add" button), "Notification settings" (with two "On" toggle switches for desktop notifications and immediate email delivery), "Language" (set to English (US)), and "Conversation settings" (with an "Edit" button). The left sidebar has navigation links for Home, Explore (Communities, Storylines), Favorites (with a "Keep your favorites at your fingertips" note), Communities (All Company, Discover communities), and Admin (Amit Ratnapara, New, ...).

I see the tenant settings

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Viva Engage tenant settings interface. At the top, it displays the user's name (Amit - 101572711) and the URL https://engage.cloud.microsoft/main/org/techsolutionsinc.store/admin/tenant-settings. The left sidebar includes sections for Home, Explore (+ Create new), Communities, Storylines, Favorites (with a note to keep favorites at fingertips), and Communities (All Company and Discover communities). The main content area is titled 'Viva Engage tenant name' and shows 'ARBC2025'. It contains several configuration sections: 'Usage policy' (Add custom usage policy, A custom usage policy has not been set up yet), 'Require users to review policy upon initial login and after updates' (Off), 'Tenant logo' (Add tenant logo), 'Notification settings' (Allow users to enable desktop notifications On, Allow community admins to enable immediate email delivery On), 'Language' (System message language: English (US)), 'Conversation settings' (Includes file formats, media, translation, and private messages), and 'Other' (Manage other tenant configurations through the Viva Engage admin center).

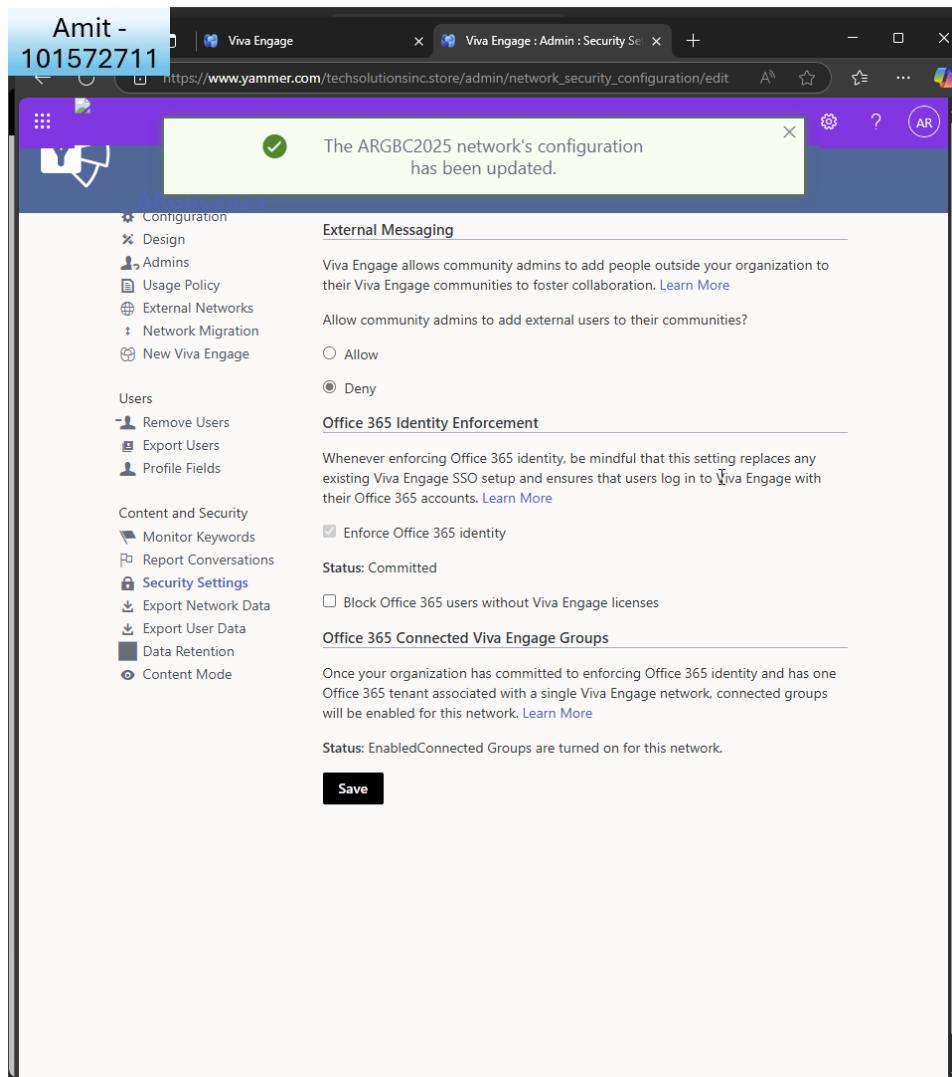
I click 'other tenant configurations' at the bottom

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



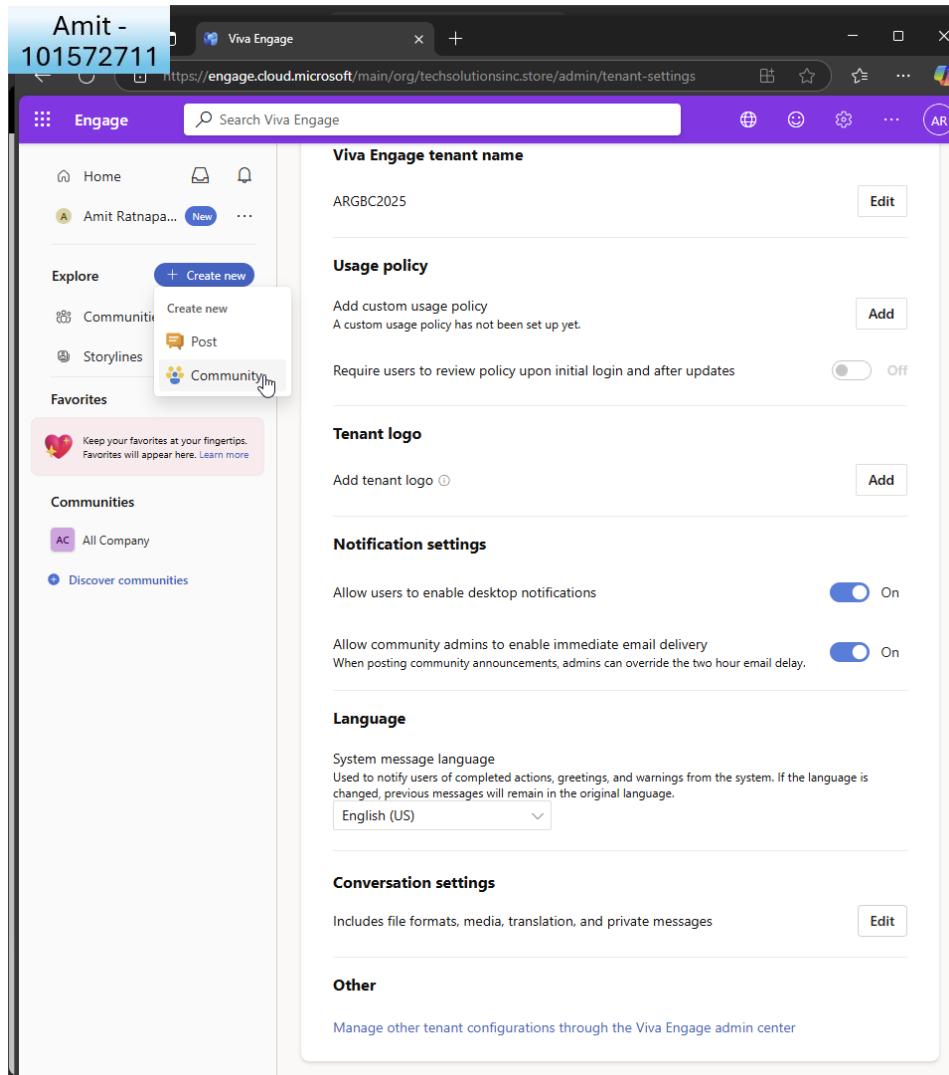
I choose to 'deny' the ability for community admins to add external users

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

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



The screenshot shows the Viva Engage tenant settings interface. On the left, there's a sidebar with options like Home, Explore, Communities, Storylines, Favorites, Communities, and Discover communities. A context menu is open over the 'Community' option in the sidebar, showing 'Create new', 'Post', and 'Community'. The main panel is titled 'Viva Engage tenant name' and shows 'ARGBC2025' with an 'Edit' button. It includes sections for 'Usage policy' (with a note that a custom usage policy hasn't been set up yet), 'Require users to review policy upon initial login and after updates' (switched off), 'Tenant logo' (with an 'Add' button), 'Notification settings' (with switches for desktop notifications and immediate email delivery both turned on), 'Language' (set to English (US)), 'Conversation settings' (with an 'Edit' button), and 'Other' (with a link to manage other tenant configurations). The browser address bar shows 'https://engage.cloud.microsoft/main/org/techsolutionsinc.store/admin/tenant-settings'.

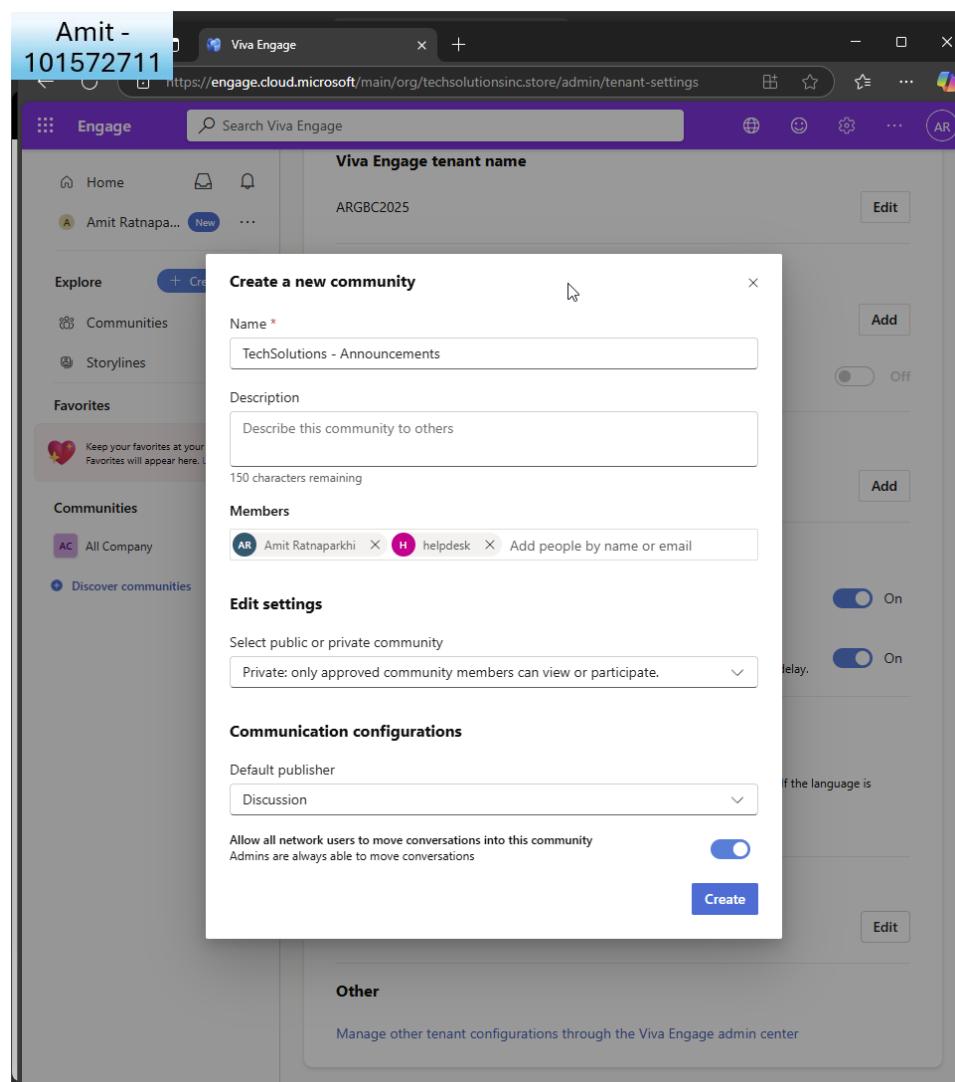
I go back to the main menu and 'create new community'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

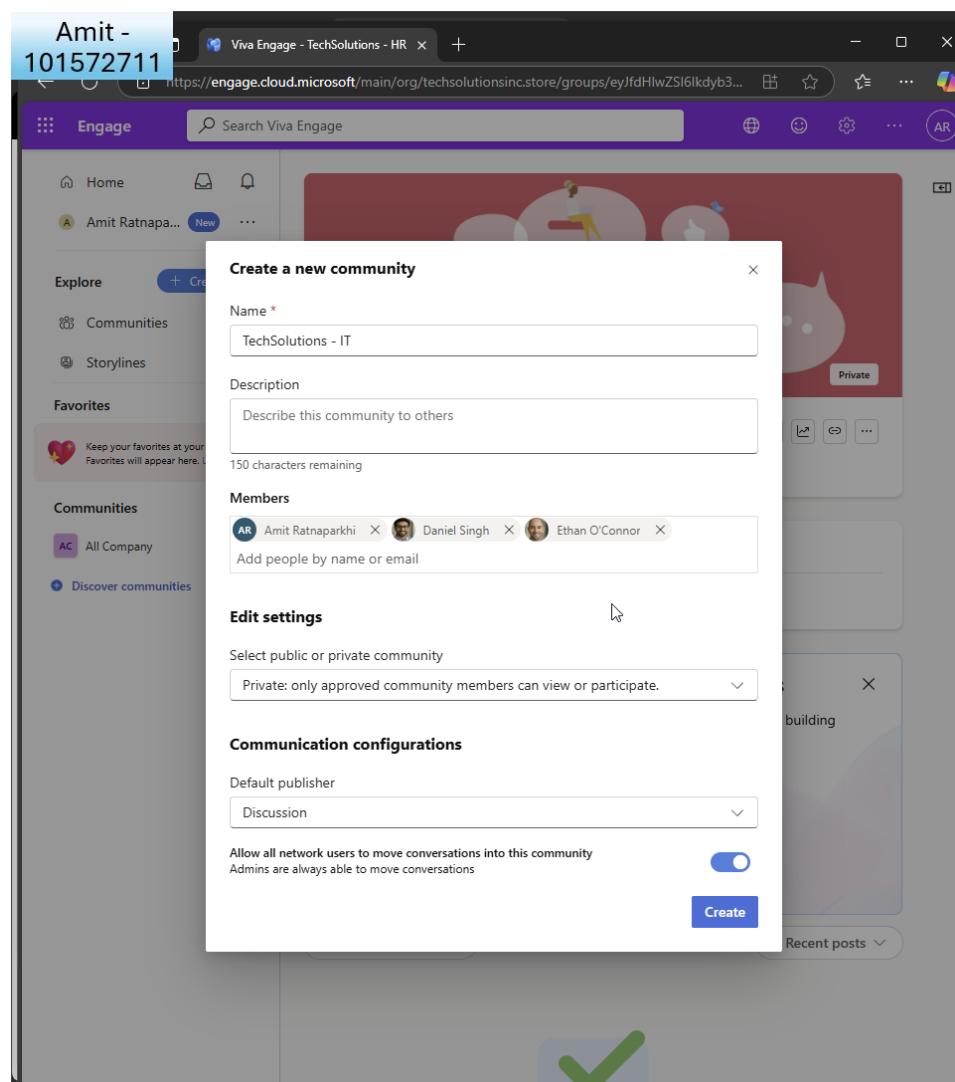


I create a new community for announcements, make it private and add GA and helpdesk

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



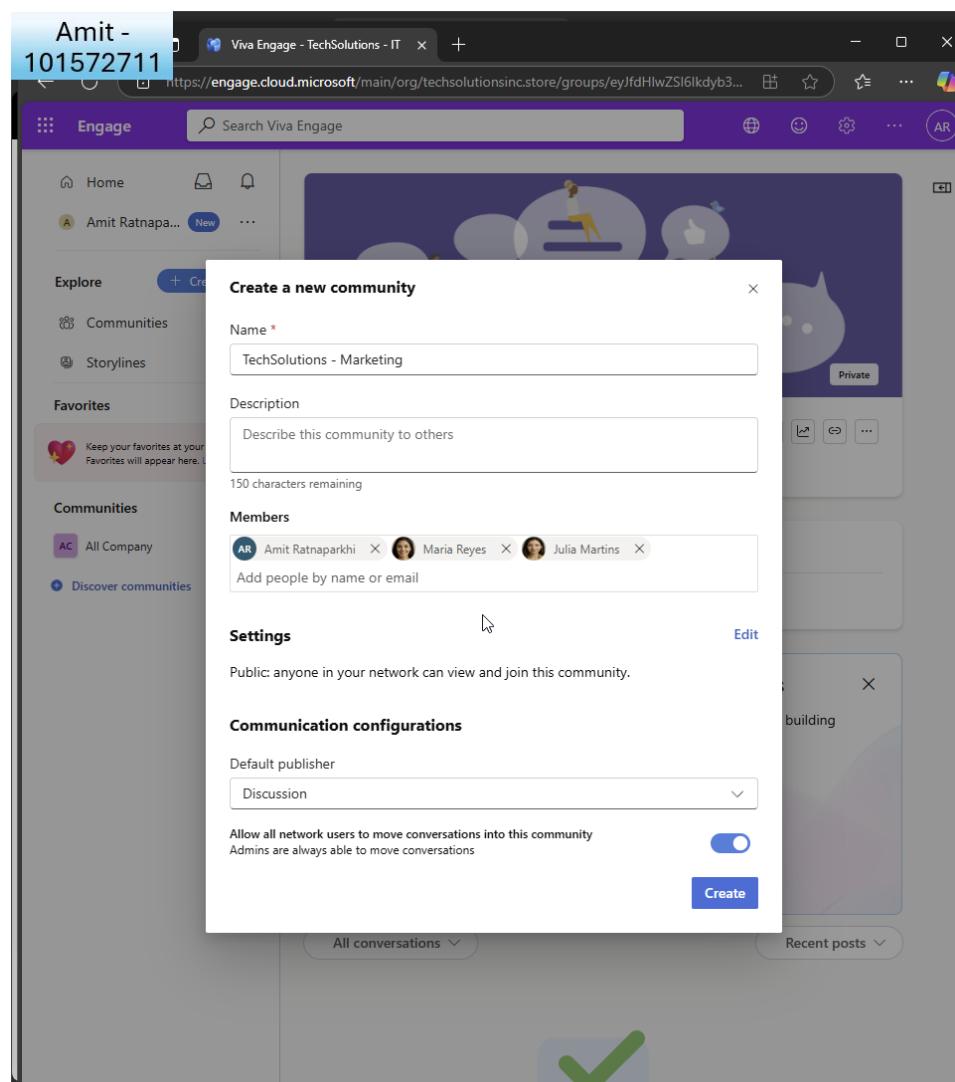
I do the same for IT department and add GA, and IT leads

Microsoft 365 Identity and Services – Enterprise Administration

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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the title bar "Amit - 101572711" and the address bar "https://www.yammer.com/techsolutionsinc.store/admin/monitor_list". The main content area is titled "Monitor Keywords". On the left, there is a sidebar with navigation links: Network (Success, Configuration, Design, Admins, Usage Policy, External Networks, Network Migration, New Viva Engage), Users (Remove Users, Export Users, Profile Fields), and Content and Security (Monitor Keywords, Report Conversations, Security Settings, Export Network Data, Export User Data, Data Retention, Content Mode). The "Monitor Keywords" section contains an "Email Address" input field with "argbc2025@argbc2025.onmicrosoft.com" and a text area for keywords. The text area lists the following words:
password
login credentials
confidential
internal only
do not share
MFA
secret
token
encryption
hate
racist
sexist
homophobic
bullying
harassment
abuse
fired
violence

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

keywords to monitor.

The screenshot shows a Microsoft Edge browser window with the URL https://www.yammer.com/techsolutionsinc.store/admin/monitor_list. The page title is "Viva Engage : Admin : Monitor Ke...". The left sidebar has sections for Network (Success, Configuration, Design, Admins, Usage Policy, External Networks, Network Migration, New Viva Engage), Users (Remove Users, Export Users, Profile Fields), and Content and Security (Monitor Keywords, Report Conversations, Security Settings, Export Network Data, Export User Data, Data Retention, Content Mode). The main content area is titled "Monitor Keywords". It includes an "Email Address" input field with the value "argbc2025@argbc2025.onmicrosoft.com" and a text area for "Enter keywords or phrases to monitor, each on its own line." A scrollable list contains the following keywords:
encryption
hate
racist
sexist
homophobic
bullying
harassment
abuse
fired
violence
GDPR
PCI
whistleblower
complaint
report HR
lawsuit
data breach
internal document

Here are some more.

Microsoft 365 Identity and Services – Enterprise Administration

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 separate 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.

Microsoft 365 Identity and Services – Enterprise Administration

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.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a 'Compliance' icon highlighted. The main content area is titled 'All admin centers'. A table lists several admin centers:

Name	Description
Dynamics 365 Apps	Use the Dynamics 365 admin center to manage your environment, manage capacity, monitor usage and perform other admin operations.
Exchange	Manage advanced email settings, such as quarantine, encryption, and mail flow rules.
Microsoft Defender ATP	Monitor and respond to security alerts on devices protected by next-generation protection, endpoint detection and response, and many other capabilities of Microsoft Defender Advanced Threat Protection.
Microsoft Defender for Identity	Identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.
Microsoft Entra	Use the Microsoft Entra admin center to manage identities, permissions, and network access.
Microsoft Intune	A single management experience for the End User Computing team in IT to ensure employees' Microsoft 365 devices and apps are secured, managed, and current.
Microsoft Purview	Use the Microsoft Purview portal to manage data security, data governance, and risk and compliance solutions for all your data, across multiple cloud platforms and apps
Office configuration	Manage, configure, and monitor deployment of Microsoft 365 Apps for your organization.
Power Automate	Manage the automation of repetitive and time-consuming tasks in the Power Platform admin center, where you can set up connections to web services, files, or cloud-based data and put them to work.
Power BI	This admin center enables Power BI service admins to manage a Power BI tenant for your organization. The portal includes items such as usage metrics and settings.
Power Platform	Secure and govern your Power Platform and Dynamics 365 products at scale. You can manage licensing and usage for apps, flows, agents, websites, and Dataverse tables, plus much more.
Search & intelligence	Manage Microsoft Search settings including services and content that are available for people in your organization. Make finding internal tools, documents, and people just as easy as searching the web in Bing.

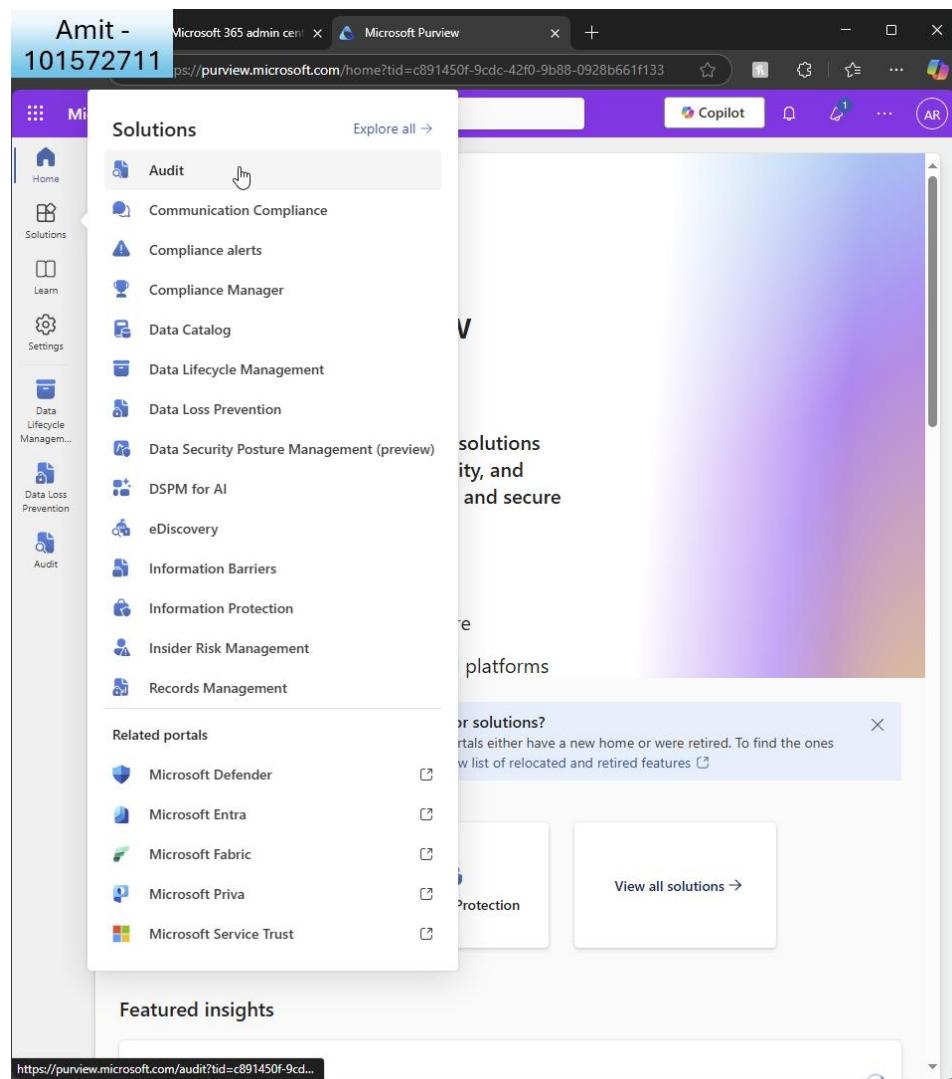
I go to the compliance centre

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



Under 'solutions' I choose 'audit'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Purview Audit search interface. The left sidebar has 'Audit' selected. The main area contains search filters for 'Start' (Apr 14 2025, 02:30) and 'End' (Apr 14 2025, 03:00). Below these are sections for 'Keyword Search' (Enter the keyword to search for), 'Admin Units' (Choose which Admin Units to search for), 'Activities - friendly names' (Modified file, Uploaded file), 'Activities - operation names' (Enter operation values, separated by commas), 'Record Types' (Select the record types to search for), 'Search name' (Give the search a name), and 'Users' (Daniel Singh, Add the users whose audit logs you want to search). A Copilot button is visible in the top right.

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

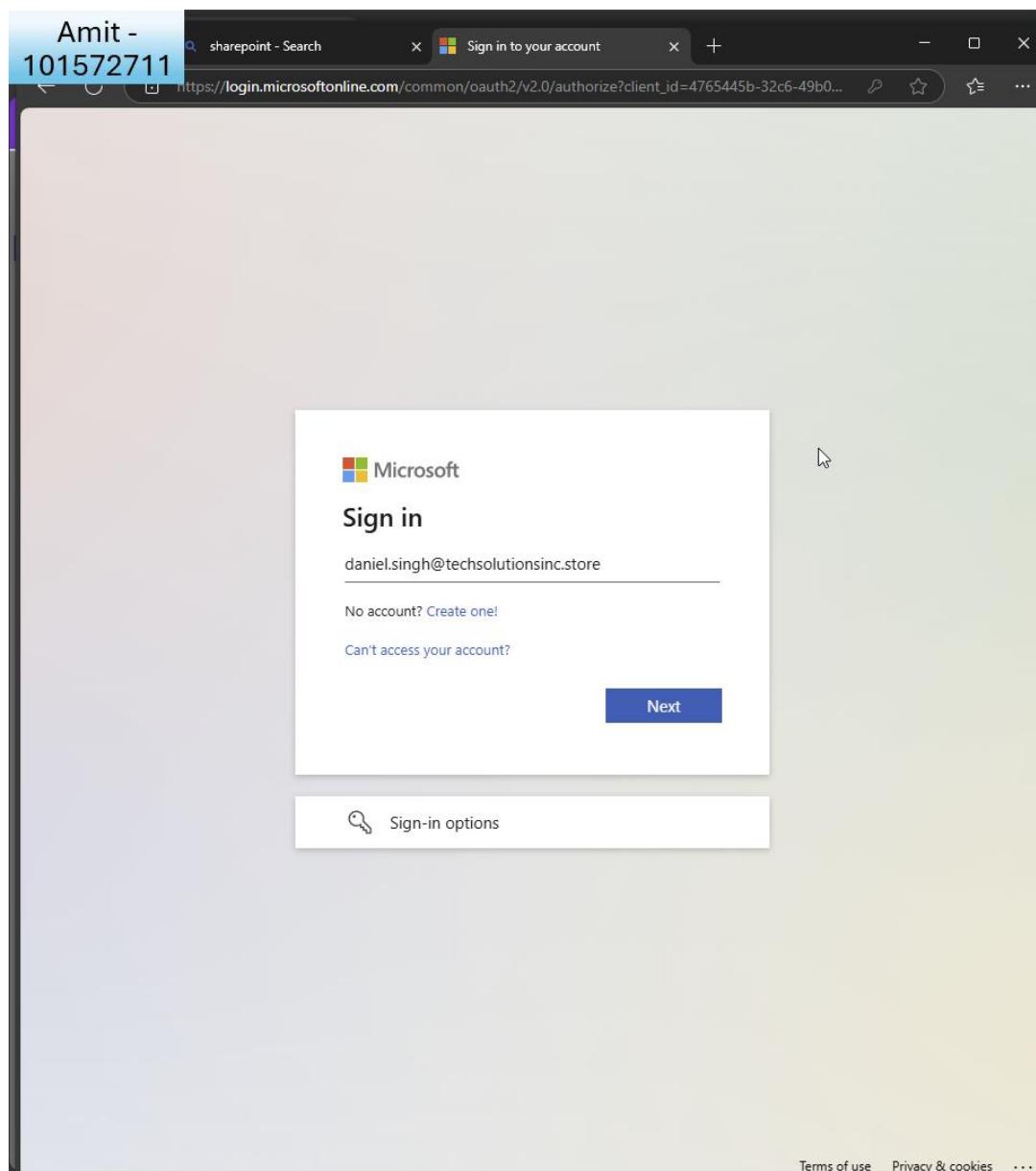
Microsoft 365 Identity and Services – Enterprise Administration

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



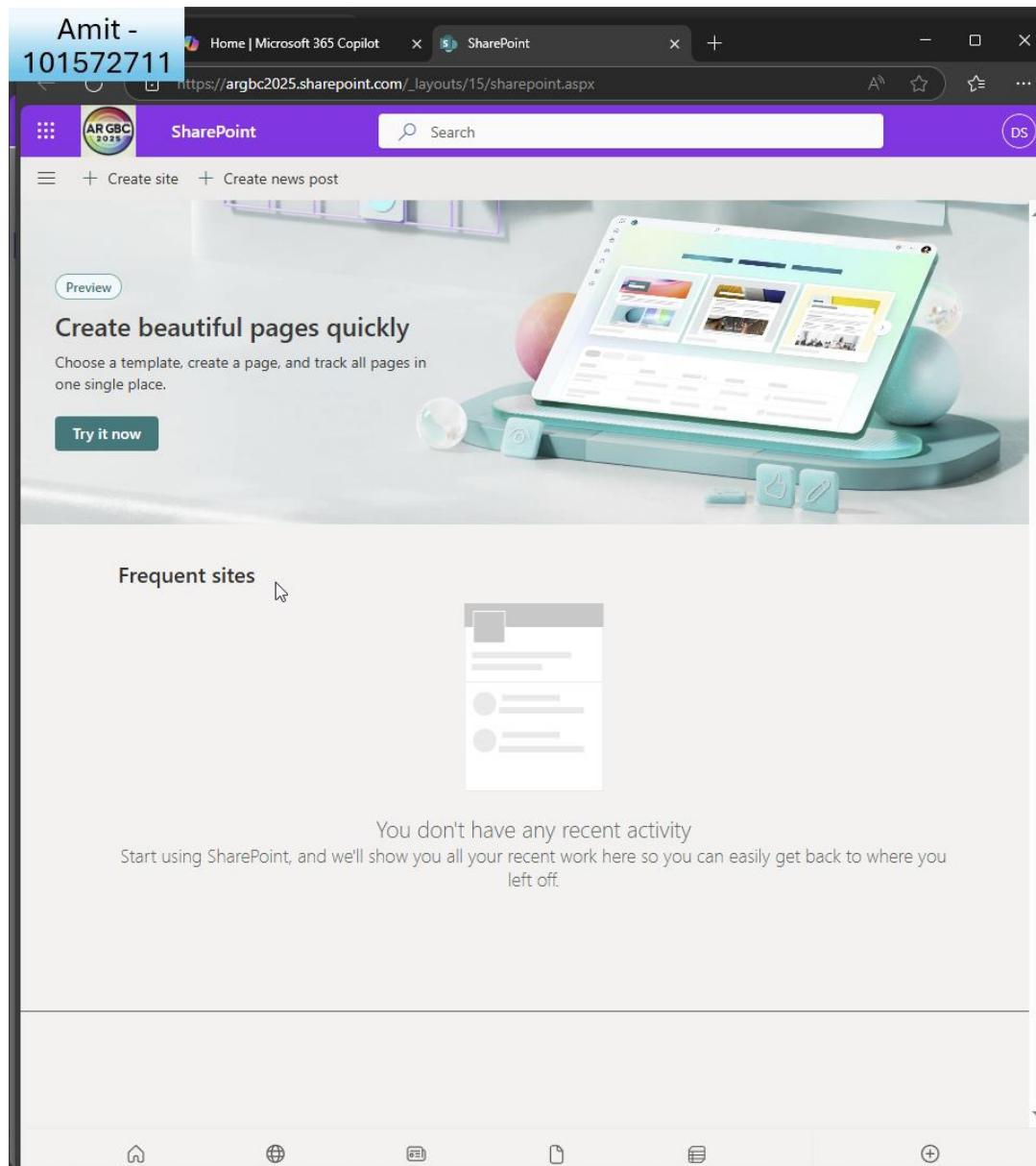
I wish to run a search for user 'Daniel' to see if he uploaded and modified a file to IT

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

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



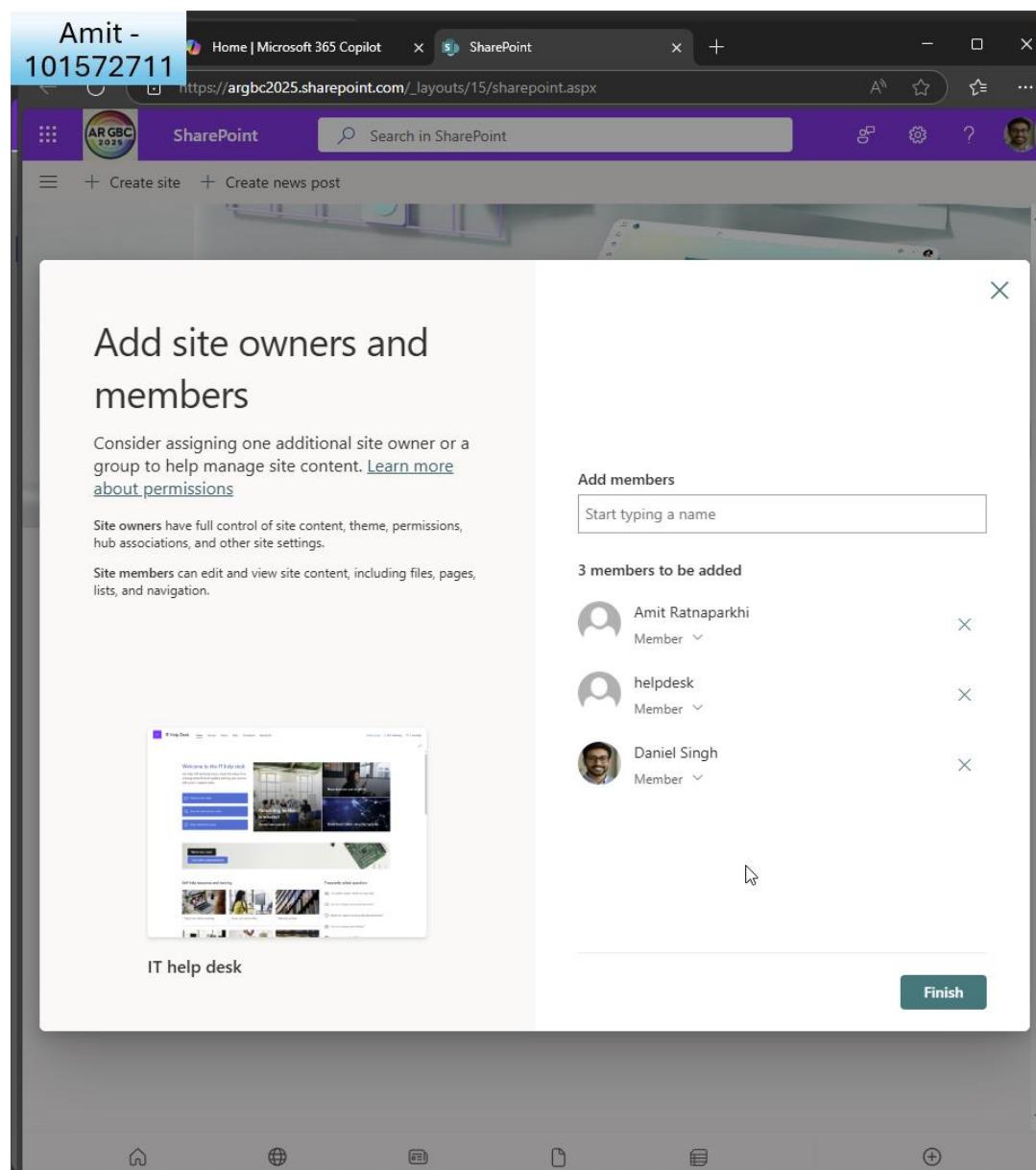
First I must create a site within IT sharepoint

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



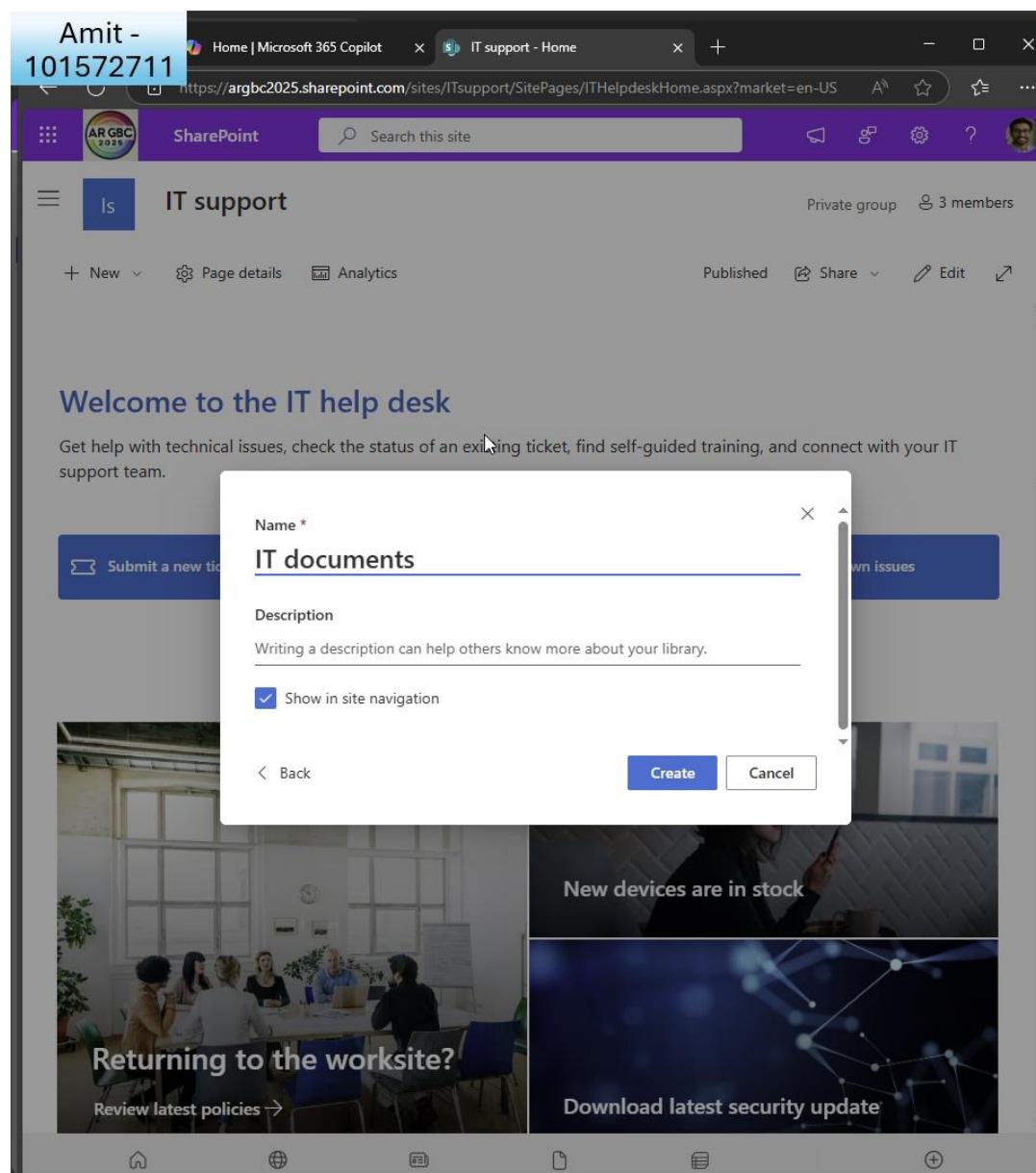
I add 'Daniel' with GA and helpdesk as members

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

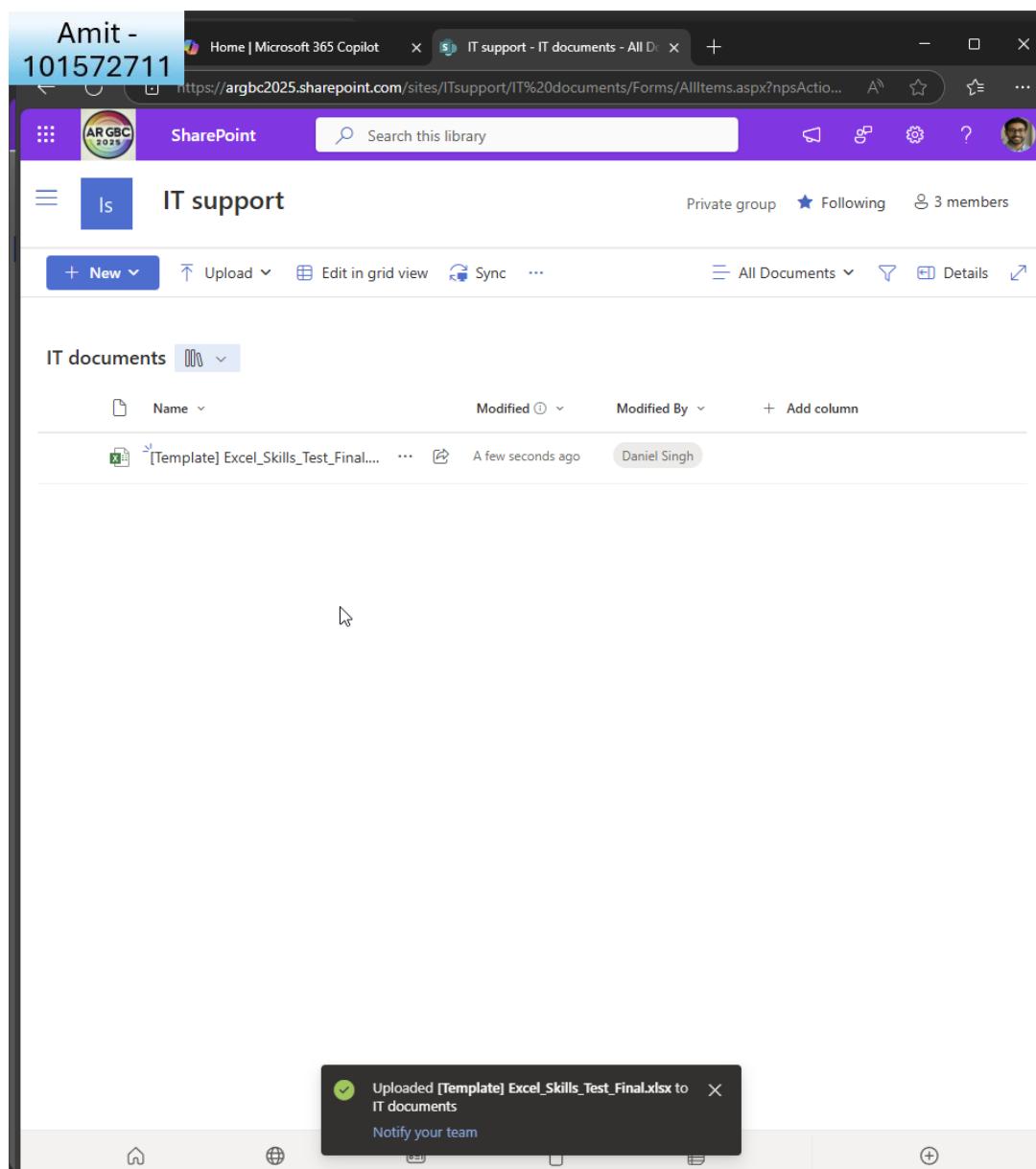


I create an 'IT documents' page

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Excel window with the title bar 'Amit - 101572711' and the URL 'https://argbc2025.sharepoint.com/:x/r/sites/ITsupport/_layouts/15/Doc.aspx?sourceid=%7BFC56...'. The Excel ribbon is visible with the 'Home' tab selected. The worksheet contains the following content:

1 Exercise 1:
2 Enter the totals using the SUM function.
3
4 A B
5 Item Quantity Cost Total
6 Apples 10 5
7 Bananas 20 6
8 Oranges 15 3
9 Total
10
11 Exercise 2:
12 Add five more items with different quantities and costs and update the total calculation.
13
14 Final
15
16
17
18
19
20

The status bar at the bottom shows tabs for 'Task 1 - Add Data', 'Task 2 - Fill Data', 'Task 3 - Split Data', 'Task 4 - Transpose Data', and 'Task 5'. It also includes 'Give Feedback to Microsoft', '100%', and zoom controls.

I modify the file

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Purview Audit search interface. The left sidebar has 'Audit' selected. The main search area has the following parameters:

- Start:** Apr 14 2025, 02:30
- End:** Apr 14 2025, 03:00
- Keyword Search:** Enter the keyword to search for
- Admin Units:** Choose which Admin Units to search for
- Activities - friendly names:** Modified file, Uploaded file
- Activities - operation names:** Enter operation values, separated by commas
- Record Types:** Select the record types to search for
- Search name:** Give the search a name
- Users:** Daniel Singh (selected)

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

~~~~~

The screenshot shows the 'Edit members of the role group' page in Microsoft Purview. On the left, there's a sidebar with 'Members' selected and 'Review and finish' as an option. The main area has a heading 'Edit members of the role group' and a sub-instruction 'Select users for this role group. Users can perform tasks that match their role group permissions. You can restrict role group permissions to apply to one or more admin units.' Below this are three buttons: 'Choose users', 'Choose groups', and 'Assign admin units'. A search bar at the top right shows 'daniel'. A modal window titled 'Choose users' is open, showing a list of users with 'Amit Ratnaparkhi' checked. At the bottom of the modal are 'Select' and 'Cancel' buttons.

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

~~~~~

This screenshot shows the same 'Edit members of the role group' page after the user 'Amit Ratnaparkhi' has been assigned. The modal window now shows '1 item' selected. The table below lists the assigned user: 'Display name' (Amit Ratnaparkhi), 'Email address' (ARGBC2025@ARGBC2025.onmicrosoft.com), 'Type' (User), and 'Admin units' (Organization). The 'Next' button is visible at the bottom.

Display name	Email address	Type	Admin units
Amit Ratnaparkhi	ARGBC2025@ARGBC2025.onmicrosoft.com	User	Organization

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

I assign the role to GA

The screenshot shows the Microsoft Purview Role groups for Microsoft Purview settings page. The 'Compliance Administrator' role group is selected. The 'Members' section is checked, and the 'Review and finish' section is also present. A large list of roles is displayed on the right, including Data Classification Feedback Reviewer, Data Connector Admin, Data Investigation Management, Data Map Reader, Device Management, Disposition Management, DLP Compliance Management, Hold, IR Compliance Management, Information Protection Admin, Information Protection Analyst, Information Protection Reader, Insider Risk Management Admin, Insights Reader, Manage Alerts, Organization Configuration, Purview Agent Analysis, Purview Copilot Workspace Contributor, RecordManagement, Retention Management, Scan Reader, Scan Writer, Scope Manager, Source Reader, and Source Writer. At the bottom of the screen, there are 'Back', 'Save', and 'Cancel' buttons.

I click 'save'

The screenshot shows the Microsoft Purview Role groups for Microsoft Purview settings page after saving the 'Compliance Administrator' role group. A prominent green checkmark icon and the text 'You successfully updated the role group' are displayed. Below this, a note states 'It might take up to an hour for the roles included in this role group to be fully assigned to all members.' A 'Next step' section titled 'Notify members' is shown, with a note about letting members know about their inclusion in the role group. At the bottom of the screen, there is a 'Done' button.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

I see the confirmation

The screenshot shows the Microsoft Purview Audit search interface. The left sidebar includes Home, Solutions (Audit selected), Learn, Settings, Data Lifecycle Management, and Data Loss Prevention. The main area has sections for Start (Apr 13 2025, 00:00) and End (Apr 16 2025, 01:00). It features a Keyword Search input, Admin Units dropdown, Activities - friendly names dropdown (Accessed file, Modified file, Uploaded file), Activities - operation names input (Enter operation values, separated by commas), Record Types dropdown, Search name input (Apr 13 - Apr 16 daniel.singh fileaccessed,filemodified,fileuploaded), and a Users section with Daniel Singh added.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

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

The screenshot shows the Microsoft Purview Audit search interface. The search query information is displayed as follows:

Search Query Information: Sun, 13 Apr 2025 00:00:00 GMT
to Wed, 16 Apr 2025 01:00:00 GMT , fileaccessed,
filemodified, fileuploaded ,
daniel.singh@techsolutionsinc.store , ,

Total Result Count: 58 items

The results table has columns: Date (UTC), IP Address, User, Record Type, and Activity. The data is as follows:

Date (UTC)	IP Address	User	Record Type	Activity
Apr 15, 2025 11...	198.96.84.204	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	40.82.190.28	daniel.singh@tec...	SharePointFileOp...	Modified file
Apr 15, 2025 3...	40.82.190.28	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	20.48.238.117	daniel.singh@tec...	SharePointFileOp...	Modified file
Apr 15, 2025 3...	62.3.36.38	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	40.82.191.50	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	20.48.238.117	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	62.3.36.38	daniel.singh@tec...	SharePointFileOp...	Uploaded file
Apr 15, 2025 3...	62.3.36.38	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	62.3.36.38	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	2a01:111:f402:f15...	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	2a01:111:f402:f15...	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	2a01:111:f402:f15...	daniel.singh@tec...	SharePointFileOp...	Accessed file
Apr 15, 2025 3...	2a01:111:f402:f15...	daniel.singh@tec...	SharePointFileOp...	Accessed file

I receive the results

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview Audit Results page. The top navigation bar includes 'Microsoft 365 admin center' and 'Audit Results | Microsoft Purview'. The left sidebar has 'Audit' selected, with sub-options 'Search', 'Policies', and 'Related solutions'. The main content area displays a 'Details' section for a specific audit log entry. The entry details are as follows:

- Date (UTC)**: 2025-04-15T23:25:14
- IP Address**: 198.96.84.204
- Users**: i0h.f|membership|100320048164f342@live.com
- Activity**: FileAccessed
- Item**: [https://argbc2025.sharepoint.com/sites/ITsupport/IT documents/\[Template\]](https://argbc2025.sharepoint.com/sites/ITsupport/IT documents/[Template])
Excel_Skills_Test_Final.xlsx
- AppAccessContext**:

```
{ "ClientAppId": "4765445b-32c6-49b0-83e6-1d93765276ca", "ClientAppName": "OfficeHome", "CorrelationId": "23df94a1-f0e9-6000-cec4-7173f8791471" }
```
- CreationTime**: 2025-04-15T23:25:14
- Id**: fe2394a5-aa2e-4bb7-5b9e-08dd7c74c6c1
- Operation**: FileAccessed
- OrganizationId**: (not visible)

A blue 'Close' button is at the bottom right of the modal.

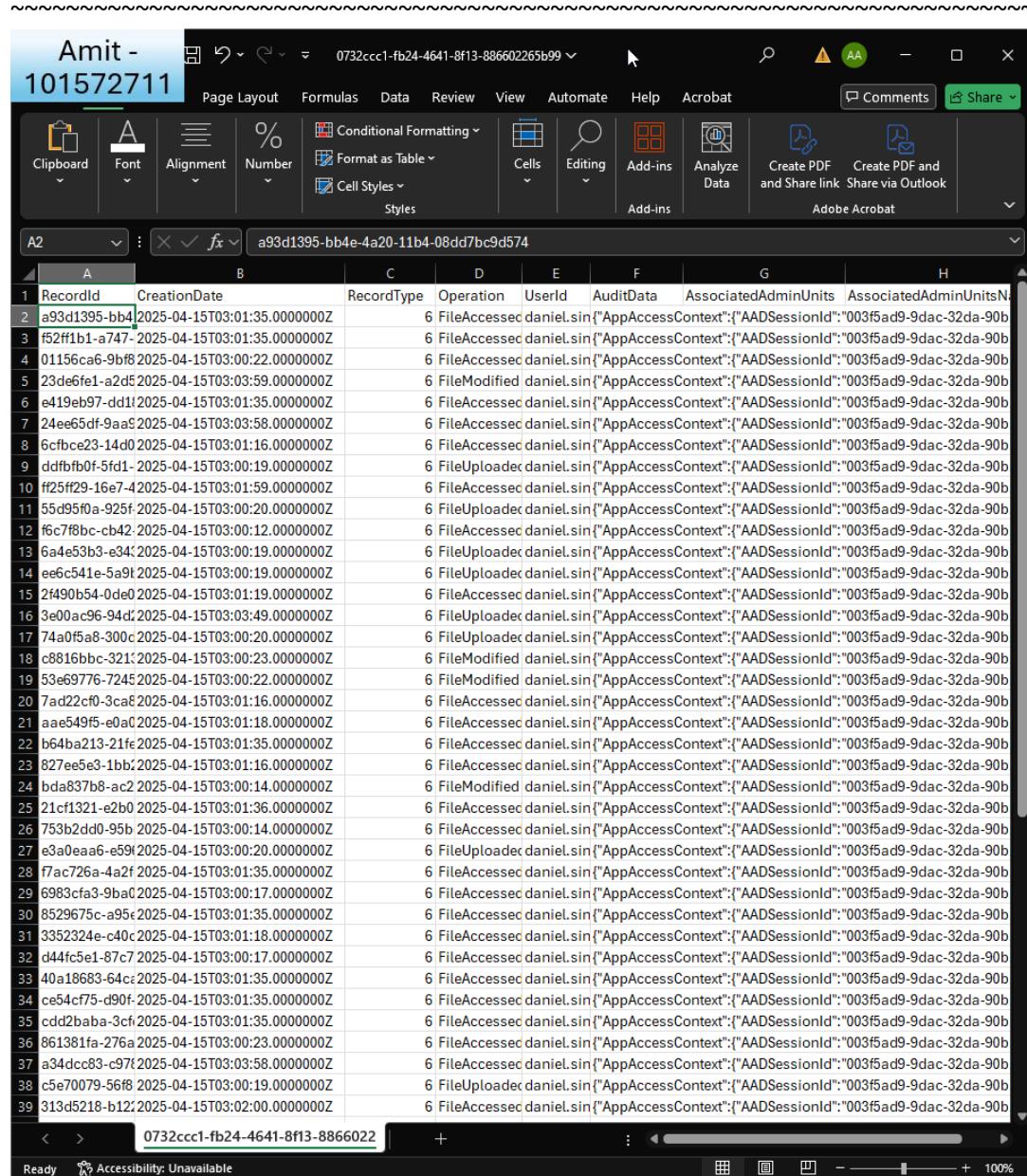
I click on the latest, for example

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



The screenshot shows a Microsoft Excel spreadsheet titled "Amit - 101572711". The window title bar indicates the file path: "0732ccc1-fb24-4641-8f13-886602265b99". The ribbon menu includes "Page Layout", "Formulas", "Data", "Review", "View", "Automate", "Help", "Acrobat", "Comments", and "Share". The toolbar contains icons for Clipboard, Font, Alignment, Number, Conditional Formatting, Format as Table, Cell Styles, Cells, Editing, Add-ins, Analyze Data, Create PDF and Share link, and Share via Outlook. The status bar at the bottom shows "Ready" and "Accessibility: Unavailable". The data is presented in a table with columns A through H. Column A contains row numbers from 1 to 39. Column B contains Record IDs. Column C contains Creation Dates. Column D contains Record Types. Column E contains Operation details. Column F contains User IDs. Column G contains Audit Data. Column H contains Associated Admin Unit IDs. The data consists of 39 rows of log entries, each detailing a specific event such as file access or modification.

A	B	C	D	E	F	G	H
1	RecordId	CreationDate	RecordType	Operation	UserId	AuditData	AssociatedAdminUnits
2	a93d1395-bb4	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
3	f52ff1b1-a747-2025-04-15T03:01:35.000000Z		6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
4	01156ca6-9bf8-2025-04-15T03:00:22.000000Z		6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
5	23de6fe1-a2d5-2025-04-15T03:03:59.000000Z		6 FileModified	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
6	e419eb97-dd1	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
7	24ee65df-9aa	2025-04-15T03:03:58.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
8	6cfbc23-14d	2025-04-15T03:01:16.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
9	ddfbfb0f-5fd1	2025-04-15T03:00:19.000000Z	6 FileUploaded	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
10	f25f29-16e7-42025-04-15T03:01:59.000000Z		6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
11	55d95f0a-925f	2025-04-15T03:00:20.000000Z	6 FileUploaded	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
12	f6c7f8bc-cb42	2025-04-15T03:00:12.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
13	6a4e53b3-e34	2025-04-15T03:00:19.000000Z	6 FileUploader	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
14	ee6e541e-5a91	2025-04-15T03:00:19.000000Z	6 FileUploader	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
15	f2490b54-0de0	2025-04-15T03:01:19.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
16	3e00ac96-94d	2025-04-15T03:03:49.000000Z	6 FileUploader	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
17	74a0f5a8-300	2025-04-15T03:00:20.000000Z	6 FileUploader	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
18	c8816bbc-321	2025-04-15T03:00:23.000000Z	6 FileModified	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
19	53e69776-7245	2025-04-15T03:00:22.000000Z	6 FileModified	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
20	7ad22cf0-3ca8	2025-04-15T03:01:16.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
21	aae549f5-e0a	2025-04-15T03:01:18.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
22	b64ba213-21fe	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
23	827ee5e3-1bb	2025-04-15T03:01:16.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
24	bda837b8-ac2	2025-04-15T03:00:14.000000Z	6 FileModified	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
25	21cf1321-e2b0	2025-04-15T03:01:36.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
26	753b2dd0-95b	2025-04-15T03:00:14.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
27	e3a0eaa6-e59	2025-04-15T03:00:20.000000Z	6 FileUploaded	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
28	f7acf26a-4a2f	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
29	6983cfa3-9ba	2025-04-15T03:00:17.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
30	8529675c-a95	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
31	3352324e-c40c	2025-04-15T03:01:18.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
32	d44fc5e1-87c7	2025-04-15T03:00:17.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
33	40a18683-64cc	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
34	ce54cf75-d90f	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
35	cdd2bab-a3cf	2025-04-15T03:01:35.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
36	861381fa-276a	2025-04-15T03:00:23.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
37	a34dcc83-c97	2025-04-15T03:03:58.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
38	c5e70079-56f8	2025-04-15T03:00:19.000000Z	6 FileUploaded	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			
39	313d5218-b12	2025-04-15T03:02:00.000000Z	6 FileAccessed	daniel.sin("AppAccessContext":{ "AADSessionId": "003f5ad9-9dac-32da-90b			

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

2. Set Up Alerts:

- Configure alert policies to notify administrators of suspicious activities, such as multiple failed login attempts or mass deletion of files.

Display name ↑	Username	Licenses
101572711	101572711@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Aisha Chen	aisha.chen@techsolutionsinc.store	Microsoft 365 E5 (no Team)
Alice Walker	alice.walker@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Amit Ratnaparkhi	ARGBC2025@ARGBC2025.onmicrosoft.com	Microsoft Power Apps for Automate Free , Microsoft
Bob Carter	bob.carter@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Daniel Singh	daniel.singh@techsolutionsinc.store	Microsoft 365 E5 (no Team)
dynamicUser1	dynamicUser1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Ethan O'Connor	ethan.oconnor@techsolutionsinc.store	Microsoft 365 E5 (no Team)
Exchange-Admin	Exchange-Admin@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Fatima Khan	fatima.khan@techsolutionsinc.store	Microsoft 365 E5 (no Team)
GBTTESTSHARED1	GBTTESTSHARED1@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
helpdesk	helpdesk@ARGBC2025.onmicrosoft.com	Microsoft 365 E5 (no Team)
Julia Martins	julia.martins@techsolutionsinc.store	Microsoft 365 E5 (no Team)
Leo Adams	leo.adams@techsolutionsinc.store	Microsoft 365 E5
Malik Carter	malik.carter@techsolutionsinc.store	Microsoft 365 E5
Maria Reyes	maria.reyes@techsolutionsinc.store	Microsoft 365 E5

I go to Defender

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for managing alerts. The left sidebar has a dark theme with white icons and text. The 'Alerts' item is currently selected, indicated by a blue highlight. The main pane is titled 'Alerts' and displays a list of three alerts. Each alert entry includes a checkbox, the alert name ('Mail forwarding'), a severity indicator (two yellow squares followed by the word 'Medium'), and a timestamp ('2023-09-12 10:30:00'). A search bar at the top right allows filtering by name or ID.

Alert name	Tags	Severity
Mail forwarding		Medium
Mail forwarding		Medium
Anomalous Token		Medium

I create a policy for an alert

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Defender interface within the Microsoft 365 admin center. The left sidebar navigation includes 'Devices', 'Identities', 'Applications' (with 'Endpoints', 'Vulnerability management', 'Partners and APIs', 'Configuration management'), 'Identities' (with 'Service accounts', 'Health issues', 'Tools'), 'Email & collaboration' (with 'Investigations', 'Explorer', 'Review', 'Campaigns', 'Threat tracker', 'Exchange message trace', 'Attack simulation training'), and 'Policies & rules'. The main content area is titled 'Alerts' and displays three alerts: 'Mail forwarding' (Severity: Medium), 'Mail forwarding' (Severity: Medium), and 'Anomalous Token' (Severity: Medium). A 'Filter set' dropdown is open, showing options like 'Add filter', 'Alert name', 'Tags', and 'Severity'. The URL in the browser bar is <https://security.microsoft.com/alerts?tid=c891450f-9cdc-42f0-9b88-0928b661f133>.

I go to 'policies & rules'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a dark theme with various navigation items like Devices, Identities, Applications, Endpoints, and more. The main content area is titled "Policies & rules" and contains a sub-section for "Activity alerts". A list of items is shown, with one item named "Alert policy" highlighted by a mouse cursor. The URL in the browser bar is <https://security.microsoft.com/securitypoliciesandrules?tid=c891450f-9cdc-42f0-9b...>.

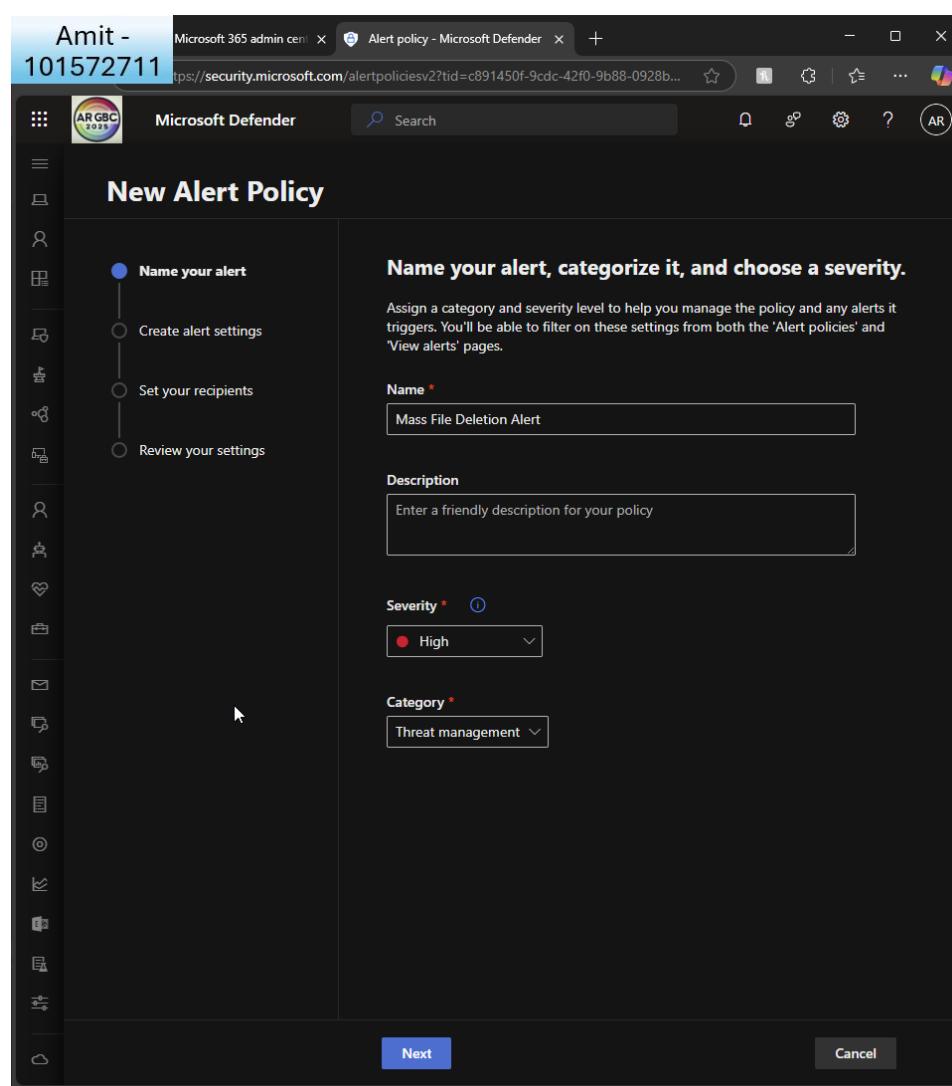
I click 'alert policy'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface for creating a new alert policy. The title bar indicates the user is 'Amit - 101572711'. The main window is titled 'Mass File Deletion Alert' and displays a step-by-step wizard:

- Step 1: Name your alert (checkbox checked)
- Step 2: **Create alert settings** (checkbox selected)
- Step 3: Set your recipients
- Step 4: Review your settings (checkbox unselected)

The 'Create alert settings' step is currently active, showing the configuration details:

Choose an activity, conditions and when to trigger the alert

You can only choose one activity but you can add conditions to refine what we'll detect.

What do you want to alert on?

Activity is: Deleted file (User deletes a document from a site)

AND

User: User is: Equal (Daniel Singh) Select an option

Add condition

Trigger an alert when the volume of matched activities are:

More than or equal to 3 activities
During the last 9999 minutes

Buttons at the bottom: Back, Next, Cancel

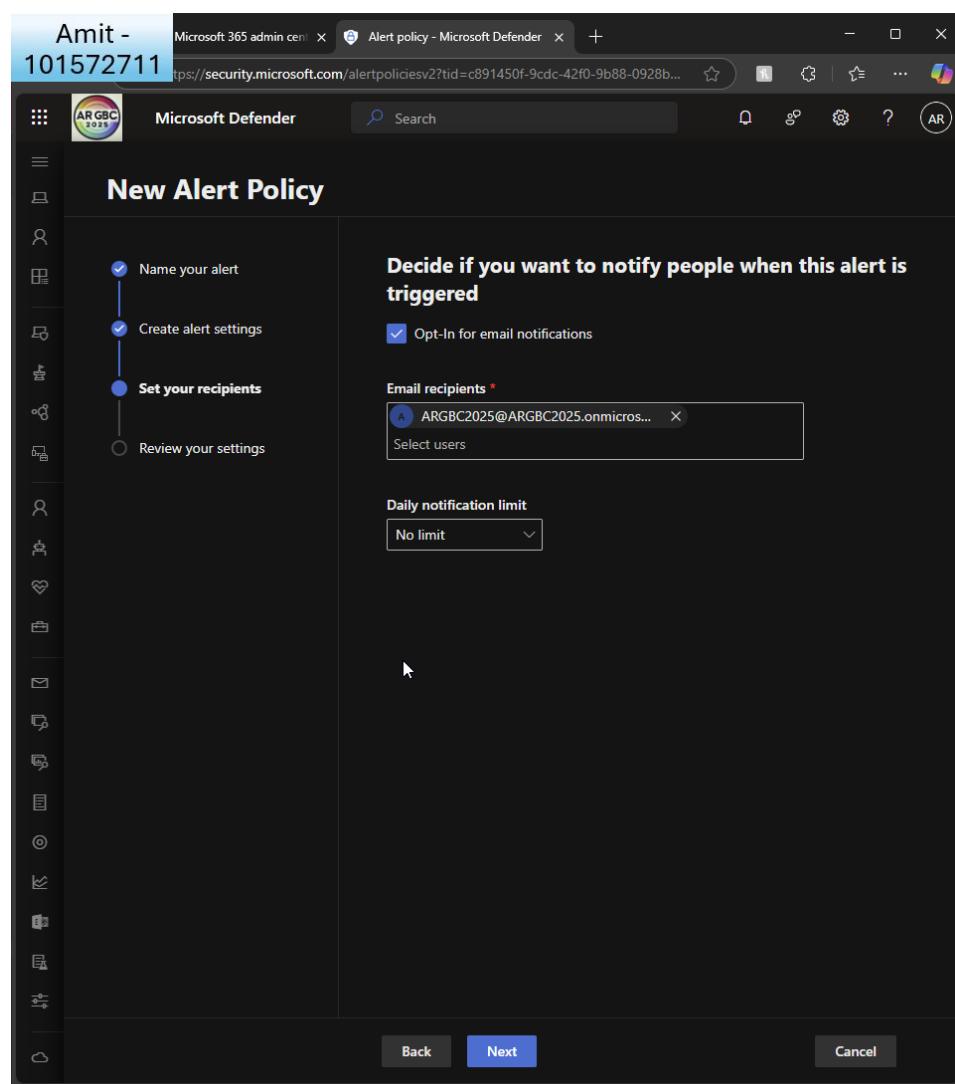
I choose to create a policy alert if files are deleted by user 'Daniel Singh'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



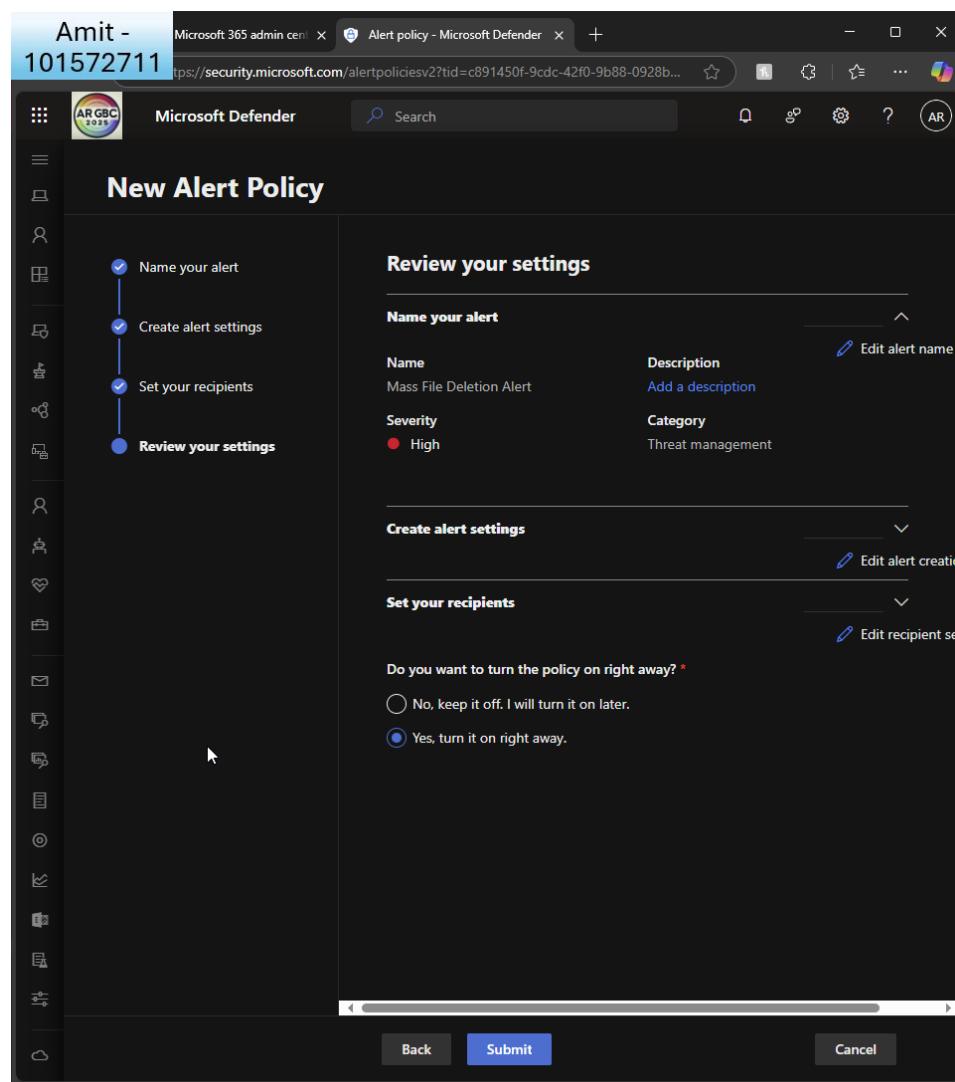
I set GA as a recipient of notification

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I review settings and turn it on straight away

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a dark theme with various navigation items like Devices, Identities, Applications, Endpoints, Vulnerability management, Partners and APIs, Configuration management, Identities, Service accounts, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, and Cloud apps. The main content area is titled 'Alert policy' and displays a list of alerts. A blue banner at the top states: 'Mail flow alerts have moved to the new Exchange admin center. Starting Oct 2021, customers will only be able to create/view/edit mail flow alerts in the new Exchange admin center.' Below the banner is a search bar and a table with columns for Name, Severity, and Type. The table lists several alerts:

Name	Severity	Type
Mass File Deletion Alert	High	Custom
Alert - Inbox Rule Created (Forwarding)	Medium	Custom
Mail forwarding	Medium	Custom
MIP AutoLabel simulation completed	Low	System
Suspicious email sending patterns detected	Medium	System
Email messages removed after delivery	Informational	System
Email messages from a campaign removed after delivery	Informational	System
Admin triggered user compromise investigation	Medium	System
User clicked through to a potentially malicious URL	High	System
Suspicious connector activity	High	System
Successful exact data match upload	Low	System
Administrative action submitted by an Administrator	Informational	System

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'.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Defender Home page. On the left, there is a navigation sidebar with the following sections:

- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules
- Cloud apps
- Cloud discovery
- Cloud app catalog
- OAuth apps
- Activity log
- Governance log
- Policies (selected)
- Policy management
- Policy templates
- Reports
- Audit
- Health
- Permissions
- Settings
- More resources

The main content area displays the following information:

- Home** section with a banner: "Get your SIEM and XDR in one place". It also mentions "Connect Microsoft Sentinel and Microsoft Defender XDR to unify your security operations in a single portal with more AI, automation, search, and threat intelligence." A "Connect a workspace" button is present.
- Microsoft Secure Score** section: "Secure Score: 51.44%" (200.09/389 points achieved). It includes a chart showing the score over time from 03/24 to 04/17, with a current score of 82.7%.
- Navigation links at the bottom: Guided tour, What's new?, Community, Add cards.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 admin center interface. The left sidebar has a dark theme with various navigation options under categories like Email & collaboration, Cloud apps, Policies, Reports, Audit, Health, and Permissions. The main content area is titled "Policy templates". It features a search bar with the term "mass down" entered. Below the search bar are filter options: "Name contains mass down" and "Advanced filters". A table lists a single policy template: "Mass download by a single user". The table includes columns for "Template", "S.↓", "Linked...", "Publis...", and a date "Jan 8, 2024 ...".

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with categories like Email & collaboration, Cloud apps, Policies, Reports, Audit, Health, and Permissions. The main area is titled 'Create activity policy - Microsoft' and shows a form for defining a new policy. The policy name is 'Mass download by a single user'. The 'Policy severity' is set to 'Medium' and the 'Category' is 'Threat detection'. The 'Description' field contains the text: 'Alert when a single user performs more than 10 downloads within 1 minute.' Below this, under 'Create filters for the policy', there are two options: 'Single activity' (selected) and 'Repeated activity'. The 'Single activity' option is described as 'Every activity that matches the filters'. The 'Repeated activity' option is described as 'Repeated activity by a single user'. At the bottom, there's a section titled 'Activities matching all of the following' with several filter conditions. One condition is highlighted: 'User' equals 'Daniel Singh (daniel.singh@techsolutionsinc.store)' and 'as' 'Any role'.

I edit the policy to target user 'Daniel'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar contains navigation links for Email & collaboration, Cloud apps, Policies, Reports, Audit, Health, and Permissions. The main area is titled "Create activity policy - Microsoft" and shows a complex query builder. The query consists of several conditions:

- User does not equal External users as Actor only
- IP address Tag does not equal Microsoft Azure
- User Name is set as Any role
- User Name equals Daniel Singh (daniel.singh@techsolutionsinc.store) as Any role

Below the query builder, there are sections for "Alerts" and "Governance actions". Under "Alerts", there is a checked checkbox for "Create an alert for each matching event with the policy's severity" with options to "Save as default settings" or "Restore default settings". There is also a checked checkbox for "Send alert as email" with a recipient field "argbc2025@argbc2025.onmicrosoft.com" and a dropdown for "Daily alert limit per policy" set to 5. Under "Governance actions", there are two radio button options: "All apps" (selected) and "Microsoft 365". At the bottom, a note states "We secure your data as described in our [privacy statement](#) and [online service](#)" with "Create" and "Cancel" buttons.

I make sure GA gets sent the alert

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a dark theme with various navigation options: Email & collaboration (Email, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training), Cloud apps (Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log), Policies (Policy management, Policy templates), Reports, Audit, Health, and Permissions. The main content area is titled 'Policies' and shows a list of policies. At the top of the list are two entries: 'Mass download' and 'Alert when a si...'. Both entries have a status of '0 activ...' and a severity of 'High'. The first entry was created on 'Apr 17, ...' and the second on 'Apr 18, ...'. There are filters at the top for 'Name', 'Type' (set to 'Activity policy'), 'Status' (set to 'ACTIVE'), 'Severity' (a red bar indicating high severity), and 'Category' (set to 'Select risk category'). Below the filters are buttons for 'Create policy', 'Export', and 'Table settings'.

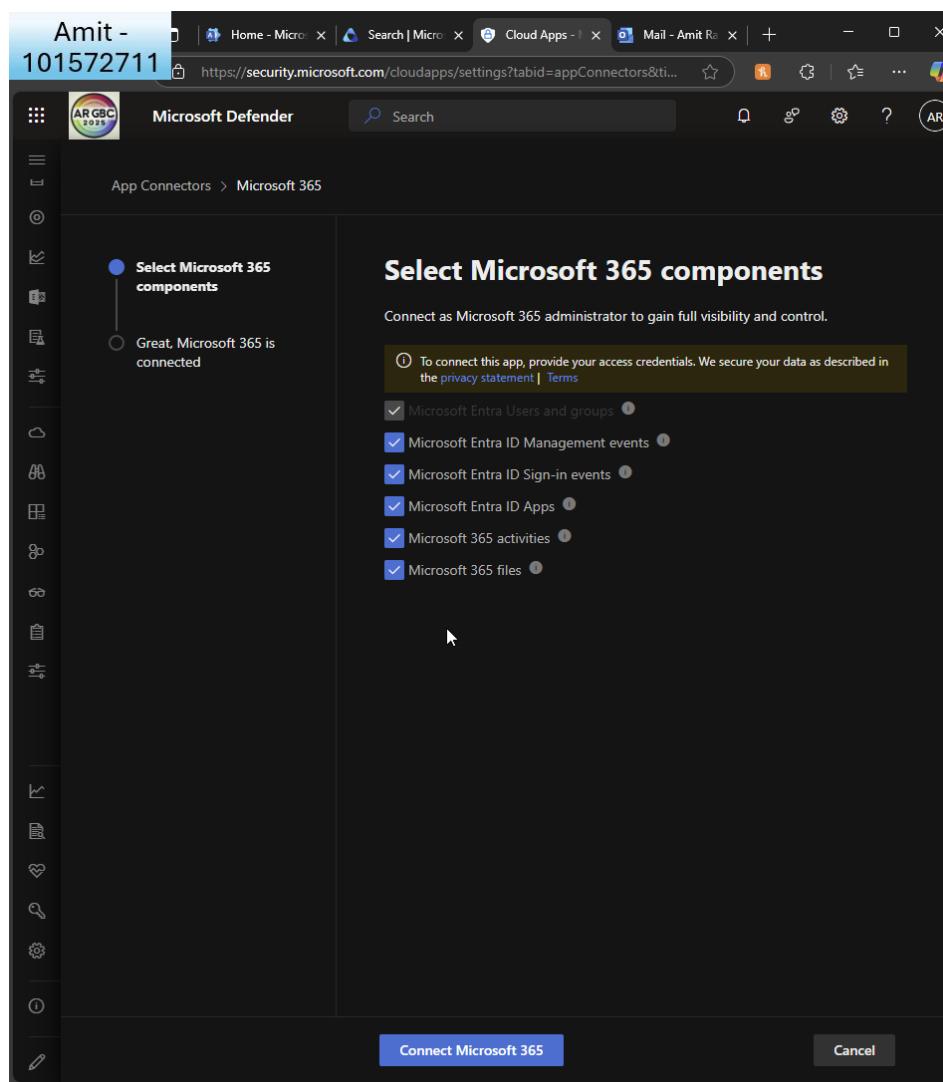
I can see my new policy listed

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



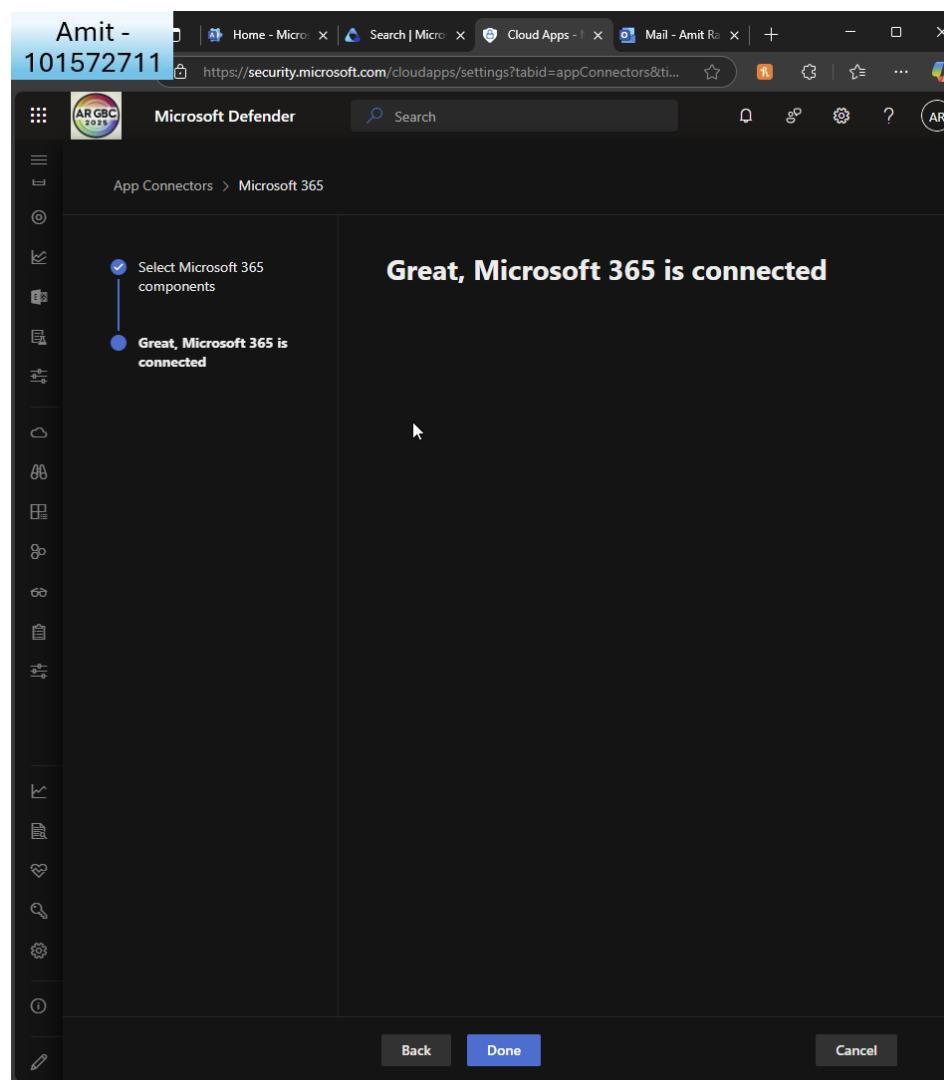
The alert was not showing in 'activity logs' so I ensured that the app connector was active for MS365 components

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I see MS365 is now connected

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender for Cloud Apps interface. The left sidebar has sections for Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps (with sub-options like Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, Policies, Policy management, Policy templates), Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main area shows the Microsoft 365 Collaboration settings under Cloud apps. The top navigation bar includes Home, Search, App Dashboard, Mail, and other tabs. The Alerts tab is selected. Filters for Status (Open/Closed), Category (Select risk category), Severity (Low/Medium/High/Critical), User name (Select users), and Policy (Select policy) are present. Below the filters is a Bulk selection dropdown, Export button, Hide filters button, and Table settings dropdown. A large bell icon with a cursor arrow over it is centered in the main content area. Text below the bell says "Phew, you have no open alerts" and there is a "Create policy" button.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

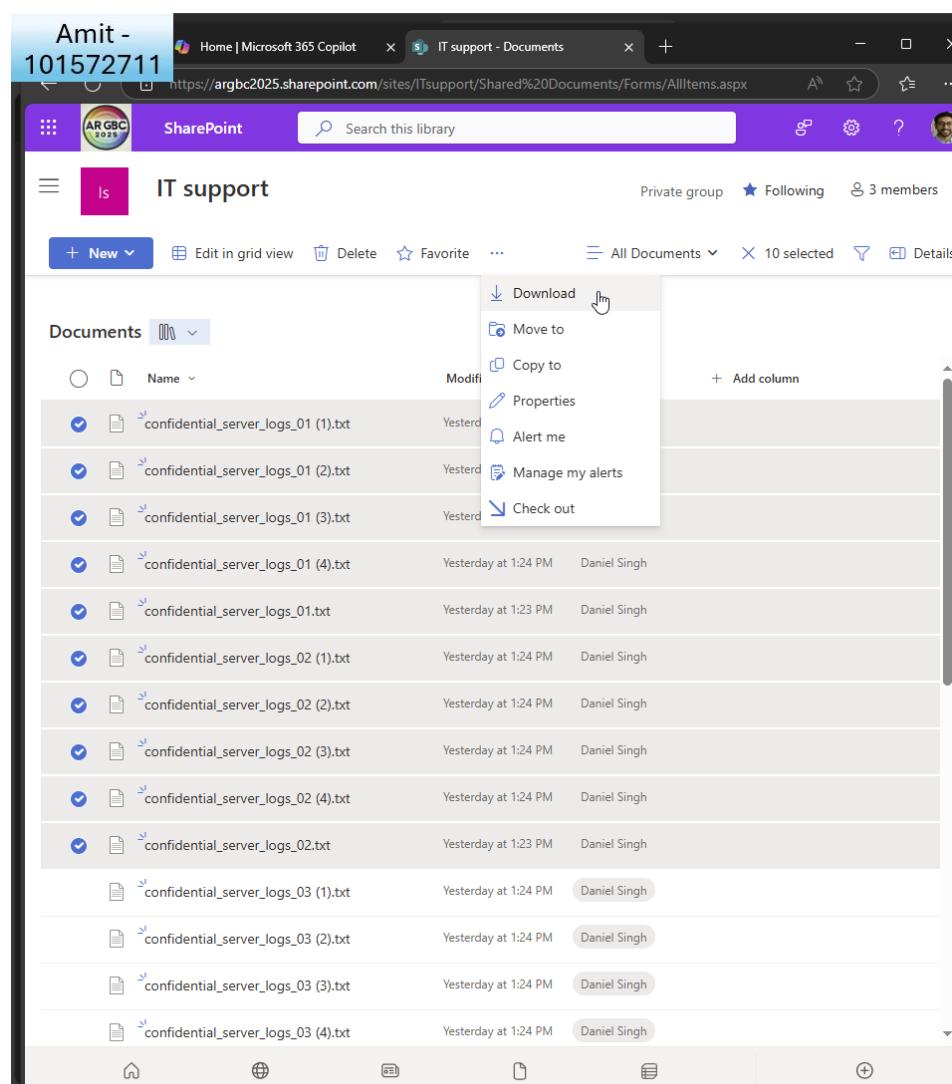
The screenshot shows the Microsoft Defender interface for creating a new activity policy. The left sidebar navigation includes sections like Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps (with sub-options like Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log), Policies, Policy management, Policy templates, Reports, Audit, Health, Permissions, Settings, More resources, and Customize navigation. The main content area is titled 'Create activity policy'. It contains fields for 'Policy template' (set to 'Mass download by a single user'), 'Policy name' (set to 'Mass download by a single user'), 'Policy severity' (set to 'Low'), 'Category' (set to 'Threat detection'), and a 'Description' box containing the text 'Alert when a single user performs more than 10 downloads within 1 minute.' Below this, the 'Create filters for the policy' section is visible, showing filter criteria for 'Activity type' (equals 'Download') and 'User' (From group does not equal 'External users' as 'Actor only'). A link 'Edit and preview results' is also present.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



I log in as Daniel and mass download files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender Activity log interface. The left sidebar contains a navigation menu with sections like Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management (with Overview, Attack surface, Exposure insights, Secure score, and Data connectors), Assets (with Devices, Identities, Applications), Endpoints, Vulnerability management, and Partners and APIs. The main area is titled 'Activity log' and includes a search bar, filter options (e.g., Matched policy, equals, Mass download by a single user), and a table header with columns for Action, User, IP address, Location, Device, and Date. A specific event is highlighted in the table, showing a download from an IP address (198.96.84...) to a device (Daniel...) on April 1st.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Defender interface with the title bar "Amit - 101572711" and the URL "https://security.microsoft.com/alerts?tid=c891450f-9cdc-42f0-9b88-0928b661f133". The left sidebar contains navigation links for Home, Incidents & alerts (selected), Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Secure score, Data connectors, Assets, Devices, Identities, Applications, and Endpoints. The main content area is titled "Alerts" and displays 10 alerts. The alerts listed are:

Alert Type	Severity
Mass download by a single user	High
Mass download by a single user	High
Mass download by a single user	High
Mass download by a single user	High
Mass download by a single user	High
Mass download by a single user	High
DLP policy (DLP - Credit Card Protection) matched...	Low
DLP policy (Canada Financial Data) matched for d...	High
Mail forwarding	Medium

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

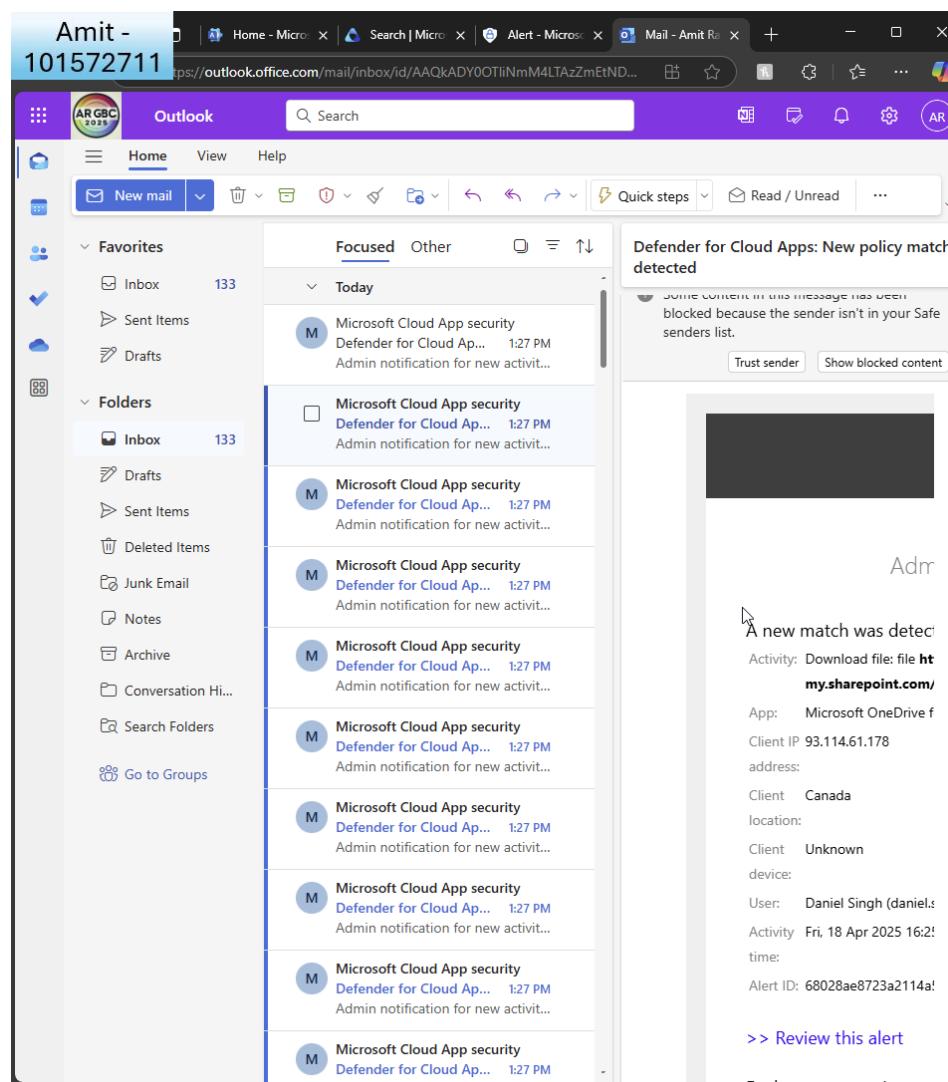
The screenshot shows the Microsoft Defender interface with a dark theme. The left sidebar contains navigation links such as Home, Incidents & alerts (with Alerts selected), Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Assets, Devices, Identities, Applications, Endpoints, and Vulnerability management. The main pane displays an alert titled "Mass download by a single user". It shows details for a user named "daniel.singh" (IP: 198.96.84.204) and an activity related to "Microsoft SharePoint Online". A tooltip labeled "Alert story" points to the "Alert story" link in the main pane. Below the alert details, there is a section titled "What happened" which states: "Activity policy 'Mass download by a single user' was triggered by 'Daniel Singh (daniel.singh@techsolutionsinc.store)'". There is also a "Related activities" section with a table showing one item: "Download file: file https... User Daniel Singh App Microsoft SharePoint Online IP address 198.96.84.204".

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



I also receive the alert as a notification to GA

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

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

The screenshot shows a Microsoft Purview interface with a sidebar and a main content area. The sidebar includes sections for Home, Solutions, Learn, Settings, and various Microsoft Entra ID and Purview services like Data connectors, Device onboarding, Optical character recognition (OCR), and Solution settings. The main content area is titled "Role groups for Microsoft Purview solutions" and displays a table of 66 items. The columns are Name, Type, and Description. The roles listed are: Organization Management, Compliance Administrator, Purview Administrators, Attack Simulator Administrators, Attack Simulator Payload Auth..., Security Administrator, Audit Manager, Billing Administrator, eDiscovery Manager, Insider Risk Management, Insider Risk Management Admin..., Insider Risk Management Anal..., Insider Risk Management Inve..., and Communication Compliance I... All roles are marked as Built-in.

Name	Type	Description
Organization Management	Built-in	
Compliance Administrator	Built-in	
Purview Administrators	Built-in	
Attack Simulator Administrators	Built-in	
Attack Simulator Payload Auth...	Built-in	
Security Administrator	Built-in	
Audit Manager	Built-in	
Billing Administrator	Built-in	
eDiscovery Manager	Built-in	
Insider Risk Management	Built-in	
Insider Risk Management Adm...	Built-in	
Insider Risk Management Anal...	Built-in	
Insider Risk Management Inve...	Built-in	
Communication Compliance I...	Built-in	

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview admin center interface. The left sidebar has a 'Settings' section expanded, showing 'Role groups' selected under 'Microsoft Entra ID'. The main content area is titled 'SOLUTIONS' and displays a list of built-in roles. One role, 'Insider Risk Management', is checked.

Name	Type	Description
Organization Management	Built-in	
Compliance Administrator	Built-in	
Purview Administrators	Built-in	
Attack Simulator Administrators	Built-in	
Attack Simulator Payload Authors	Built-in	
Security Administrator	Built-in	
Audit Manager	Built-in	
Billing Administrator	Built-in	
eDiscovery Manager	Built-in	
Insider Risk Management	Built-in	
Insider Risk Management Admins	Built-in	
Insider Risk Management Analysts	Built-in	
Insider Risk Management Investigators	Built-in	
Communication Compliance Investigators	Built-in	
Privacy Management	Built-in	
Privacy Management Administrators	Built-in	

I click it

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Insider Risk Management interface. A modal dialog titled "Choose users" is open, prompting the user to "Choose one or more users to add to the role group." The dialog includes a search bar and a list of users. One user, "Amit Ratnaparkhi", is selected, indicated by a checked checkbox. Other users listed include Exchange-Admin, sally, Toronto, Maria Reyes, Fatima Khan, 101572711, dynamicUser1, Daniel Singh, Alice Walker, Ethan O'Connor, GBTESTSHARED1, task2 user1, Malik Carter, and another Amit Ratnaparkhi entry.

Name	Email address
Exchange-Admin	Exchange-Admin@ARGBC2025.onmicrosoft.com
sally	sally@ARGBC2025.onmicrosoft.com
Toronto	Toronto@ARGBC2025.onmicrosoft.com
Maria Reyes	maria.reyes@techsolutionsinc.store
Fatima Khan	fatima.khan@techsolutionsinc.store
101572711	101572711@ARGBC2025.onmicrosoft.com
dynamicUser1	dynamicUser1@ARGBC2025.onmicrosoft.com
Daniel Singh	daniel.singh@techsolutionsinc.store
Alice Walker	alice.walker@ARGBC2025.onmicrosoft.com
Ethan O'Connor	ethan.oconnor@techsolutionsinc.store
GBTESTSHARED1	GBTESTSHARED1@ARGBC2025.onmicrosoft.com
task2 user1	user1@ARGBC2025.onmicrosoft.com
<input checked="" type="checkbox"/> Amit Ratnaparkhi	ARGBC2025@ARGBC2025.onmicrosoft.com
Malik Carter	malik.carter@techsolutionsinc.store

I choose GA as the user

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview admin center window titled "Role groups for Microsoft Purview". The URL is https://purview.microsoft.com/settings/purviewpermissions?tid=c891450f-9cdc-42f... . The main content area is titled "Insider Risk Management". On the left, there's a navigation pane with "Members" selected and "Review and finish" listed below it. The right pane is titled "Review the role group and finish". It displays the following details:

- Role group name:** Insider Risk Management
- Role group description:** -
- Roles in the role group:** Case Management, Custodian, Data Connector Admin, Insider Risk Management Admin, Insider Risk Management Analysis, Insider Risk Management Approval, Insider Risk Management Audit, Insider Risk Management Investigation, Insider Risk Management Reports Administrator, Insider Risk Management Sessions, Purview Agent Analysis, Purview Copilot Workspace Contributor, Review, View-Only Case
- Members in the role group:**

Display name	Type	Admin units
Amit Ratnaparkhi	User	Organization

At the bottom of the right pane are "Edit" and "Save" buttons, and a "Cancel" button.

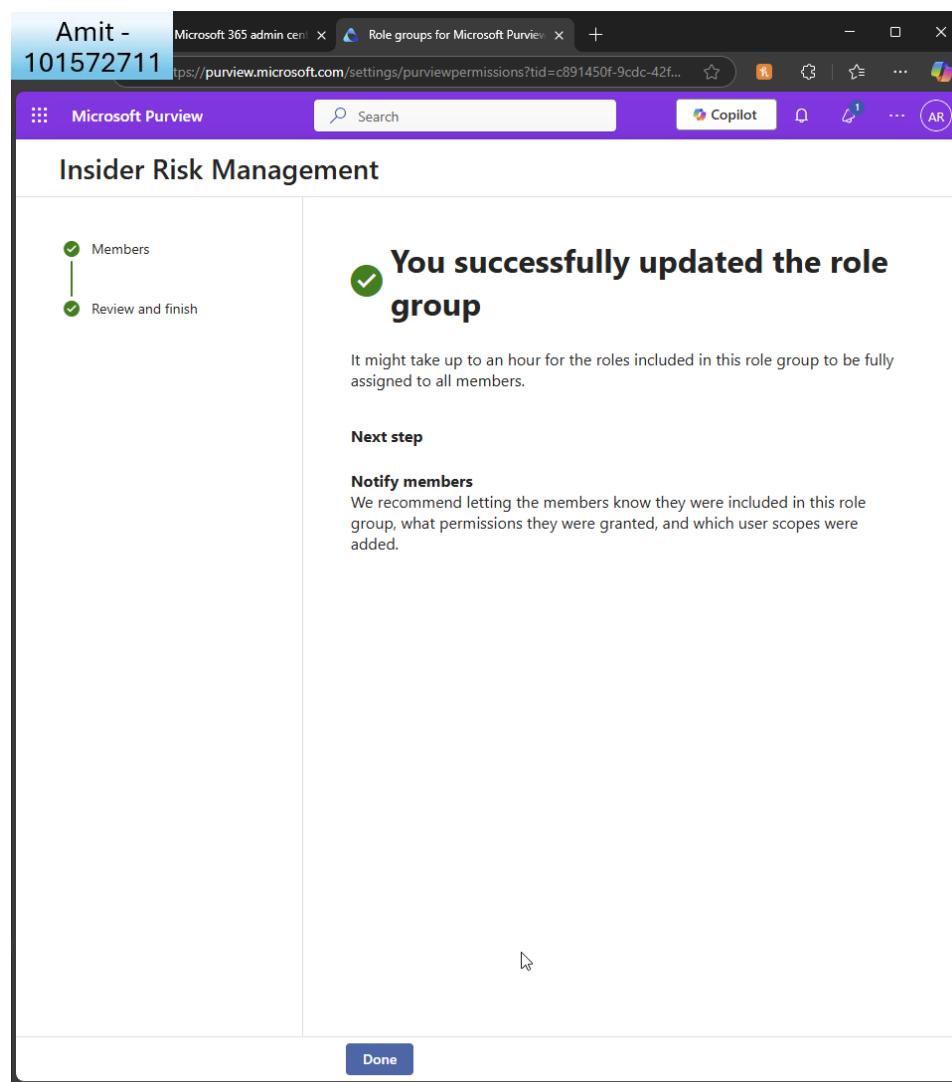
I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview Insider Risk Management Overview page. The left sidebar has a navigation menu with sections like Home, Solutions (Insider Risk Management), Learn, Recommendations, Alerts, Cases, Policies, Users, Reports, Forensic Evidence, Notice templates, Audit log, and Adaptive Protection. Below these are Related solutions for Communication Compliance, Information Barriers, and Data Loss Prevention. The main content area is titled 'Overview' and features a message: 'Amit Ratnaparkhi, here are your top recommended actions'. It lists five recommended actions:

- Turn on analytics to scan for potential risks** (Optional, 48 hours, includes video tutorial)
- Get to know insider risk management** (Optional, 10 min)
- Configure insider risk settings** (Required, 10 min, includes video tutorial)
- Create your first policy** (Required, 5 min)
- Make sure your team can get their jobs done** (Required, 10 min, includes video tutorial)

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview browser interface. The top navigation bar includes 'Amit - 101572711' and 'Overview | Microsoft Purview'. The main content area displays a message: 'Analytics scan started' with a checkmark icon. Below this, a note states: 'We're scanning recent activity in your org for potential insider risks. This might take a couple days, but you'll get an email when there are insights and policy recommendations to review. You can also check back and access your report from the Overview page.' On the left, a sidebar lists various solutions under 'Insider Risk Management': Home, Solutions (Insider Risk Management), Learn, Overview, Recommendations, Alerts, Cases, Policies, Users, Reports, Forensic Evidence, Notice templates, Audit log, and Adaptive Protection. Below this, 'Related solutions' include Communication Compliance, Information Barriers, and Data Loss Prevention.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview Policies page. The left sidebar has a navigation menu with the following items:

- Home
- Solutions
 - Insider Risk Management
 - Overview
 - Recommendations
 - Alerts
 - Cases
- Insider Risk Management
 - Policies (selected)
 - Users
 - Reports
 - Forensic Evidence
 - Notice templates
 - Audit log
 - Adaptive Protection
- Data Lifecycle Management
- Data Loss Prevention
- Audit

Below the sidebar, there's a "Related solutions" section with links to Communication Compliance, Information Barriers, and Data Loss Prevention.

The main content area is titled "Policies". It displays three metrics: Policy warnings (0), Policy recommendations (0), and Healthy policies (0). A callout box suggests turning on analytics to scan user activity daily. Below this, there's a search bar with placeholder text "Start scoring activity for users" and a "Refresh" button. The results table shows 0 items.

At the bottom right, a message says "You don't have any policies yet. We recommend starting with a basic policy." The URL in the address bar is <https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=c891450f-9cdc-42f0-9b88-0928b661f133>.

I create my policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Purview Policies page. The left sidebar has sections for Home, Solutions (Insider Risk Management, Learn, Settings), and Policies (Overview, Recommendations, Alerts, Cases, Data leaks, Users, Reports, Forensic Evidence, Notice templates, Audit log, Adaptive Protection). Below these are Related solutions: Communication Compliance, Information Barriers, and Data Loss Prevention. The main area is titled "Create quick policies" with a sub-section "Data leaks". It describes detecting potential data leaks from all users in the org. It includes a "Get started" button and a "Close" button. Other quick policy options shown include "Data theft by users leaving your org", "Critical asset protection", "Email exfiltration", and "Risky AI Usage (preview)". Each option has a "Get started" button and some are marked as "New".

I create a quick policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Policies interface. On the left, there's a sidebar with various navigation options like Home, Solutions, Learn, Recommendations, Alerts, Cases, Policies (which is selected), Users, Reports, Forensic Evidence, Notice templates, Audit log, and Adaptive Protection. Below these are Related solutions for Communication Compliance, Information Barriers, and Data Loss Prevention. The main content area is titled "Create a data leak policy". It includes a "Time to complete" section stating "2 min" and a note about data leaks ranging from accidental oversharing to theft with intent. A "How do quick policies work?" link is present. The "Policy name" field contains "Data leaks quick policy - 4/16/2025". The "User scope" dropdown is set to "Include all users and groups (Recommended for best coverage)". A "Settings we filled in for you" section notes that settings are based on a scan and can be customized. Under "Triggering event", it says "User performs an exfiltration activity". The "Indicators" section lists several SharePoint-related activities. At the bottom are "Create policy" and "Customize" buttons.

I create a 'data leak' policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft Purview Policies page. The left sidebar has a 'Policies' section selected under 'Insider Risk Management'. The main area displays policy metrics: 0 Policy warnings, 1 Policy recommendations, and 1 Healthy policies. A tooltip suggests turning on analytics to scan user activity daily. Below this, a table lists one policy item: 'Data leaks quick policy - mass file deletion' with a status of '1 recommendation'. The table has columns for 'Policy name' and 'Status'.

Policy name	Status
Data leaks quick policy - mass file deletion	1 recommendation

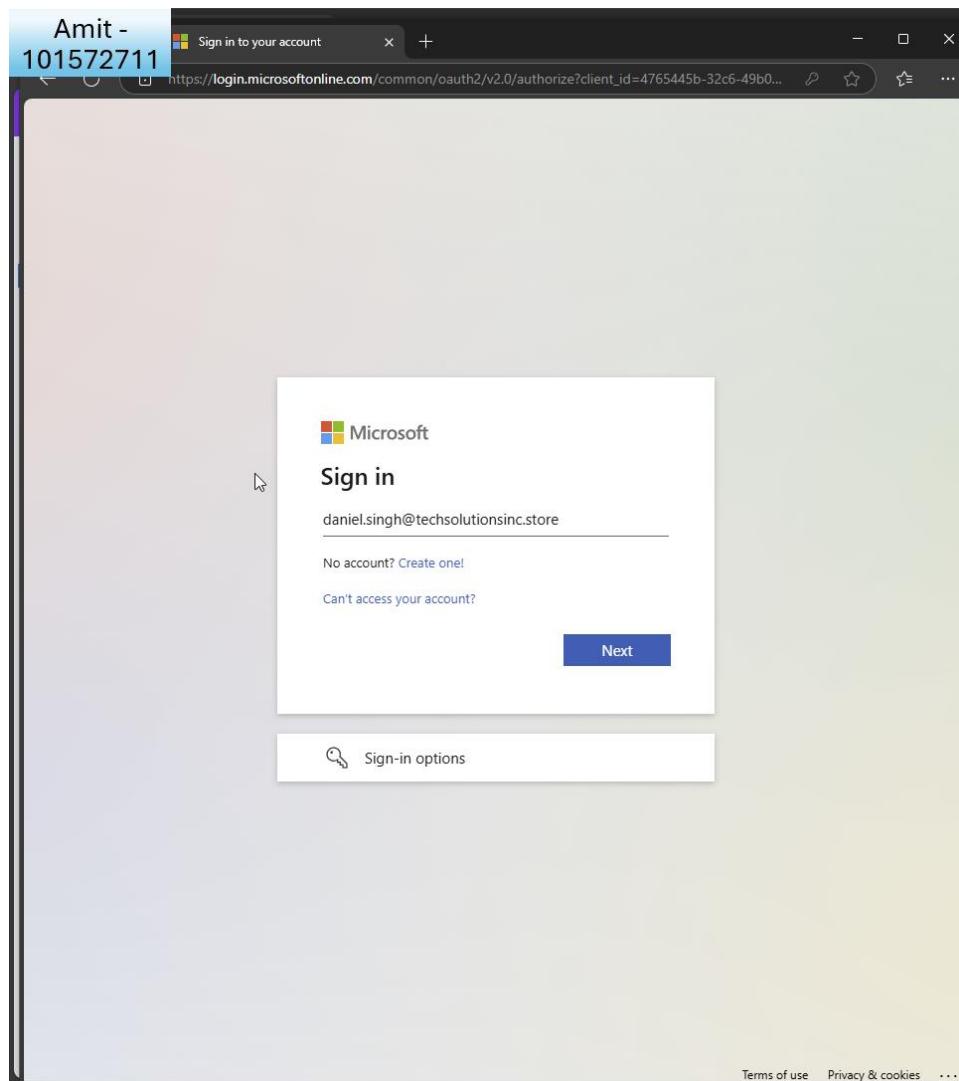
I see the new policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



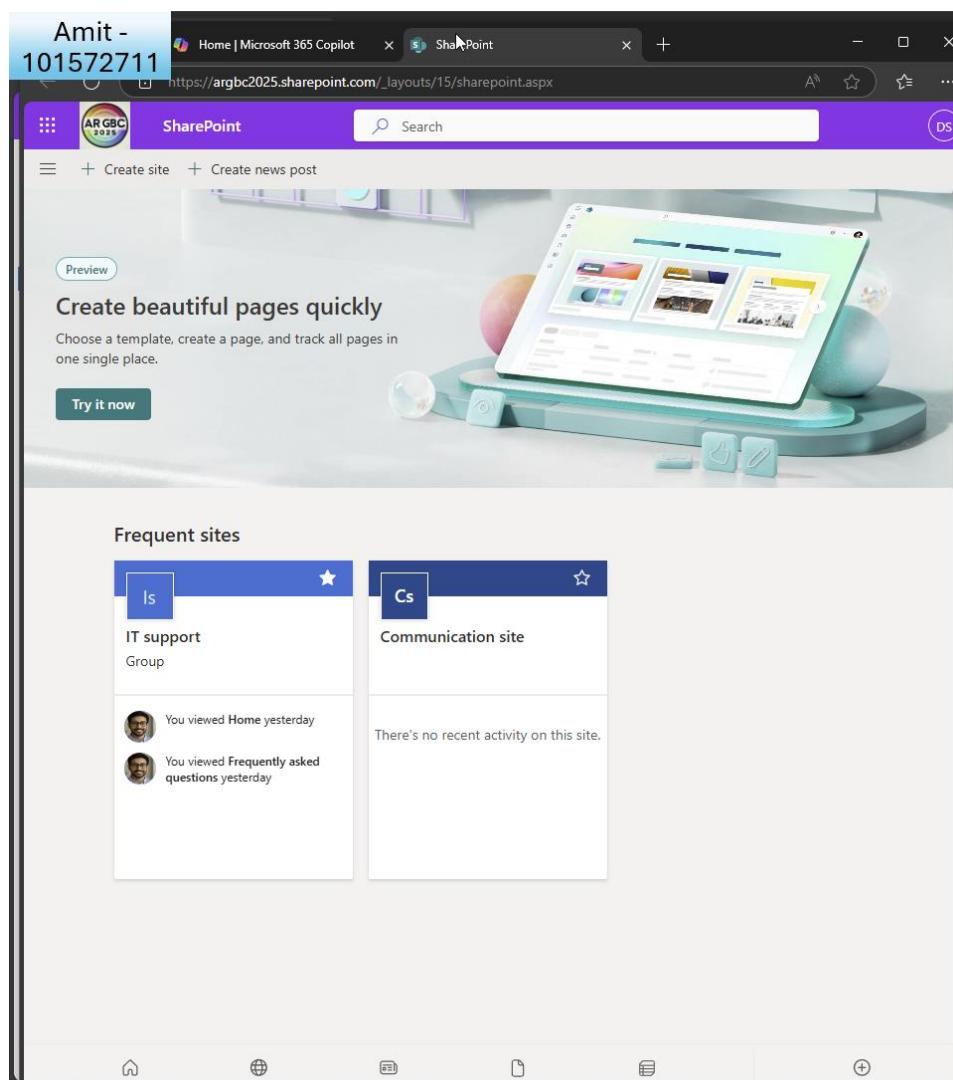
To simulate I sign in as Daniel

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I go to IT support page to upload many documents

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft SharePoint interface. At the top, there's a navigation bar with tabs for 'Home | Microsoft 365 Copilot', 'IT support - Documents - All Doc...', and a '+' button. Below the bar, it says 'Amit - 101572711' and 'SharePoint'. There's a search bar with 'Search this library' and a user profile icon. The main area is titled 'IT support' and is described as a 'Private group' with 'Following' and '3 members'. Below the title, there are buttons for '+ New', 'Upload', 'Edit in grid view', 'Sync', and more. A dropdown menu shows 'All Documents' and 'Details'. The main content is a 'Documents' list with columns for 'Name', 'Modified', and 'Modified By'. The list contains 13 items, all named 'confidential_server_logs_{number}.txt' (from 01 to 13), each modified 'A few seconds ago' by 'Daniel Singh'. At the bottom of the list, a dark overlay displays a green checkmark and the text 'Uploaded 50 items to Documents'.

Here are the files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft SharePoint document library interface. The title bar indicates the user is signed in as 'Amit - 101572711' and the library name is 'IT support'. The URL is <https://argbc2025.sharepoint.com/sites/Itsupport/Shared%20Documents/Forms/AllItems.aspx>. The library is a 'Private group' with 3 members. A grid view is selected, showing 19 documents. The columns are 'Name', 'Modified', 'Modified By', and 'Actions'. All documents are named 'confidential_server_logs_{number}.txt' where {number} ranges from 01 to 19. Each document was modified 'A few seconds ago' by 'Daniel Singh'. The 'Delete' button is highlighted with a cursor.

Name	Modified	Modified By
confidential_server_logs_01.txt	A few seconds ago	Daniel Singh
confidential_server_logs_02.txt	A few seconds ago	Daniel Singh
confidential_server_logs_03.txt	A few seconds ago	Daniel Singh
confidential_server_logs_04.txt	A few seconds ago	Daniel Singh
confidential_server_logs_05.txt	A few seconds ago	Daniel Singh
confidential_server_logs_06.txt	A few seconds ago	Daniel Singh
confidential_server_logs_07.txt	A few seconds ago	Daniel Singh
confidential_server_logs_08.txt	A few seconds ago	Daniel Singh
confidential_server_logs_09.txt	A few seconds ago	Daniel Singh
confidential_server_logs_10.txt	A few seconds ago	Daniel Singh
confidential_server_logs_11.txt	A few seconds ago	Daniel Singh
confidential_server_logs_12.txt	A few seconds ago	Daniel Singh
confidential_server_logs_13.txt	A few seconds ago	Daniel Singh
confidential_server_logs_14.txt	A few seconds ago	Daniel Singh
confidential_server_logs_15.txt	A few seconds ago	Daniel Singh
confidential_server_logs_16.txt	A few seconds ago	Daniel Singh
confidential_server_logs_17.txt	A few seconds ago	Daniel Singh
confidential_server_logs_18.txt	A few seconds ago	Daniel Singh
confidential_server_logs_19.txt	A few seconds ago	Daniel Singh

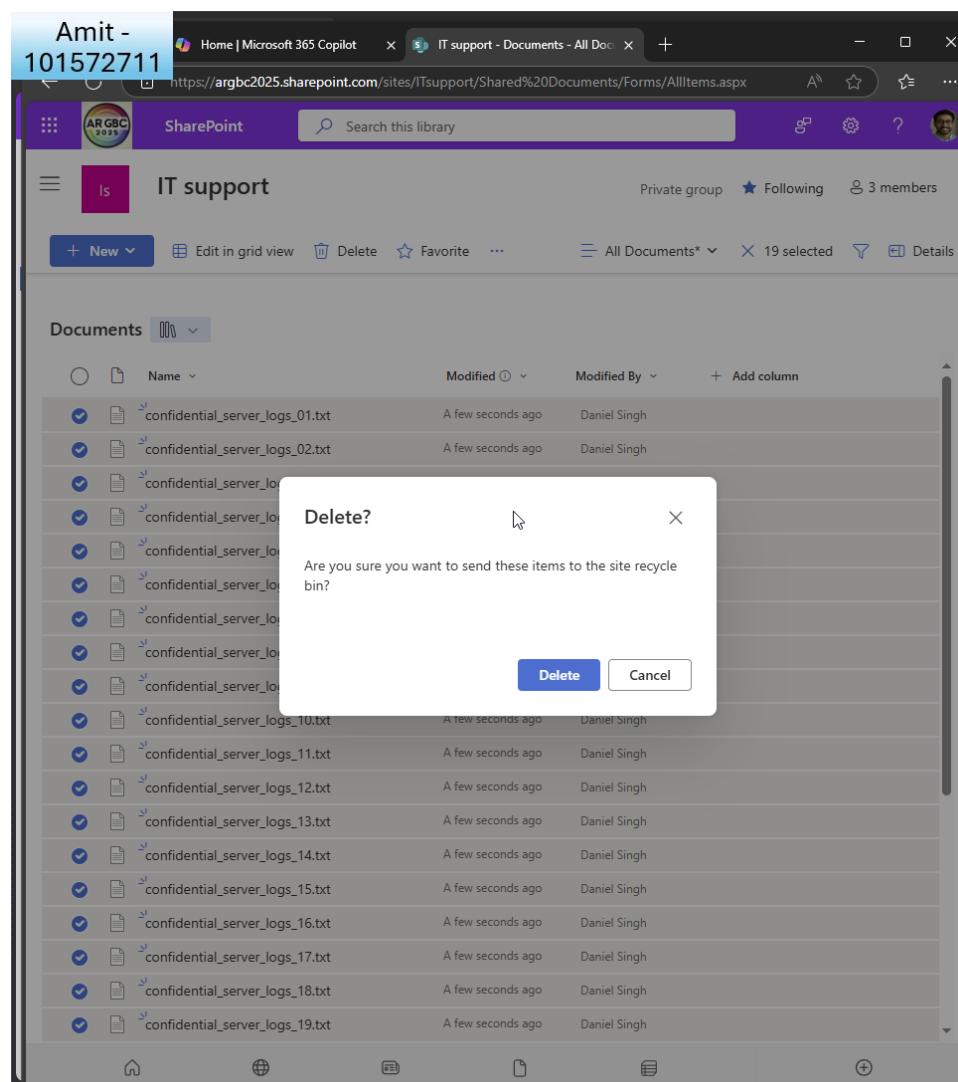
I delete multiple files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft SharePoint interface. At the top, there's a navigation bar with tabs like 'sharepoint - Search', 'Home | Microsoft 365 Co...', 'IT support', and 'Recycle bin'. Below the bar, it says 'Amit - 101572711' and shows the URL 'https://argbc2025.sharepoint.com/sites/Itsupport/_layouts/15/AdminRecycleBin.aspx?view=5'. The main area is a 'Private group' named 'IT support' with 3 members. A 'View options' dropdown is visible. The section titled 'Recycle bin' shows a table with columns: Name, Date deleted (sorted by date), Deleted by, Created by, and Original location. A message 'Your recycle bin is empty' is displayed, accompanied by a white trash can icon. At the bottom, there's a note 'Can't find what you're looking for? Check the [Second-stage recycle bin](#)'.

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:

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Purview Policies page. The left sidebar has a navigation menu with 'Data Loss Prevention' selected. Under 'Policies', there are links for 'Overview', 'Alerts', 'Classifiers', 'Explorers', and 'Diagnostics'. Below this, 'Related solutions' include 'Information Protection' and 'Insider Risk Management'. The main content area is titled 'Policies' and contains a brief description of DLP policies. It features two callout boxes: one for role group permissions and another for setting up billing in Fabric. A 'Get started' button is visible. Below these, a table lists six DLP policies with columns for Name, Priority, and Last modified. The table includes a search bar at the top.

Name	Priority	Last modified
Default Office 365 DLP policy	0	Mar 20, 2022
Default policy for devices	1	Mar 29, 2022
Default policy for Teams	2	Apr 2, 2025
DLP - Credit Card Protection	3	Apr 6, 2025
Canada Financial Data	4	Apr 10, 2022
Internal Data Loss Alerts	5	Apr 15, 2022

I create a new DLP policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create policy' wizard in Microsoft Purview. The left sidebar lists steps: 'Template or custom policy' (selected), 'Name', 'Admin units', 'Locations', 'Policy settings', 'Policy mode', and 'Finish'. The main area title is 'Start with a template or create a custom policy'. It explains that users can choose an industry regulation or start from scratch. A callout box highlights 'Check out our new enhanced policy templates', noting they extend original templates by detecting named entities like full names and physical addresses. Below this are search and filter fields ('Search for specific templates' and 'All countries or regions'). A link 'Back to Regulations' is available. Under 'U.K. Financial Data', it says this template helps detect financial information in the UK, including credit cards. A section 'Protect this information:' lists items: Credit Card Number, EU Debit Card Number, and SWIFT Code. At the bottom are 'Next' and 'Cancel' buttons.

I choose UK financial date and choose a template

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create policy' wizard in Microsoft Purview. The left sidebar lists steps: 'Template or custom policy' (checked), 'Name' (checked), 'Admin units' (checked), 'Locations' (checked), 'Policy settings' (unchecked), 'Policy mode' (unchecked), and 'Finish' (unchecked). The main pane title is 'Data loss prevention > Create policy'. It says 'We'll apply the policy to data that's stored in the locations you choose.' Below is a table of locations:

Location	Scope	Actions
Exchange email	All groups	Edit
SharePoint sites	All sites	Edit
OneDrive accounts	All users & groups	Edit
Teams chat and channel messages	Turn on location to scope	
Devices	Turn on location to scope	
Instances	Turn on location to scope	
On-premises repositories	Turn on location to scope	
Fabric and Power BI workspaces	Turn on location to scope	

At the bottom are 'Back', 'Next', and 'Cancel' buttons.

I ensure locations are correct

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a web browser window titled "Amit - 101572711" on the Microsoft Purview website. The URL is https://purview.microsoft.com/datalossprevention/policies?tid=c891450f-9cdc-42f0... The page is titled "Data loss prevention > Create policy". On the left, a vertical navigation pane lists steps: "Template or custom policy" (checked), "Name" (checked), "Admin units" (checked), "Locations" (checked), "Policy settings" (selected), "Policy mode" (unchecked), and "Finish" (unchecked). The main content area is titled "Define policy settings" and contains the following text: "Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further." Below this are two radio button options: "Review and customize default settings from the template. ⓘ Credit Card Number, EU Debit Card Number, SWIFT Code" (unchecked) and "Create or customize advanced DLP rules ⓘ" (checked). At the bottom of the content area is a cursor icon. At the very bottom of the page are three buttons: "Back", "Next", and "Cancel".

I define the policy settings and customise

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create rule' interface in Microsoft Purview. The main section is titled 'Content contains' under 'Conditions'. It lists a group named 'Credit card number' with a 'Group operator' set to 'Any of these'. Below this, there's a section for 'Sensitive info types' where 'Credit Card Number' is selected with 'High confidence' and '1 to Any' instances. There are options to 'Add' or 'Evaluate predicate for (available for Exchange workload only)'. The 'Actions' section is present but currently empty. The 'User notifications' section is also present but currently empty. At the bottom, there are 'Save' and 'Cancel' buttons.

I create the rule for credit card numbers

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create rule' interface in Microsoft Purview. The top navigation bar includes 'Home - Microsoft 365', 'Policies | Microsoft Purview', 'Mail - Amit Ratnaparkhi', and other tabs. The main area is titled 'Create rule'. It has three main sections: 'Content contains', 'Actions', and 'User overrides'. The 'Content contains' section is expanded, showing a condition where 'Group name' is 'Credit card number' and the 'Group operator' is 'Any of these'. Below this, under 'Sensitive info types', 'Credit Card Number' is listed with 'High confidence' and 'Instance count 1 to Any'. There are buttons for 'Add' and 'Evaluate predicate for (available for Exchange workload only)'. The 'Actions' section is expanded, showing an action to 'Restrict access or encrypt the content in Microsoft 365 locations'. Other actions like 'Start a Power Automate workflow' and 'Use notifications to inform your users and help educate them on the proper use of sensitive info.' are listed but disabled ('Off'). The 'User overrides' section is collapsed. At the bottom are 'Save' and 'Cancel' buttons.

I restrict access for the user

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Edge browser window with the title bar "Amit - 101572711" and the address bar "https://purview.microsoft.com/datalossprevention/policies?tid=c891450f-9cdc-42f0...". The main content is titled "Create rule". It includes sections for "Actions", "User notifications", "User overrides", and "Incident reports". The "Actions" section is expanded, showing options to "Restrict access or encrypt the content in Microsoft 365 locations". Under this, the "Block users from receiving email, or accessing SharePoint, OneDrive, and Teams files, and Fabric and Power BI items" option is selected. Below it, there are two radio button options: "Block everyone." (selected) and "Block only people outside your organization.". A "User notifications" section is collapsed, showing a toggle switch set to "Off". The "User overrides" section is collapsed, showing a checkbox for "Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.". The "Incident reports" section is collapsed, showing a dropdown menu for "Select an option". At the bottom are "Save" and "Cancel" buttons.

I choose 'block everyone'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create rule' page in the Microsoft Purview interface. At the top, there is a toggle switch labeled 'Off' with the note: 'Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.' Below this, under 'User overrides', there is a checkbox for 'Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.' Under 'Incident reports', the 'Use this severity level in admin alerts and reports:' dropdown is set to 'High'. A toggle switch for 'Send an alert to admins when a rule match occurs.' is turned 'On'. Below this, there are two options for sending email alerts: 'Send alert every time an activity matches the rule' (selected) and 'Send alert when the volume of matched activities reaches a threshold'. The 'Instances more than or equal to' field is set to '15' and the 'matched activities' field is set to '0 MB'. The 'During the last' field is set to '60 minutes'. The 'For' field is set to 'All users'. A toggle switch for 'Use email incident reports to notify you when a policy match occurs.' is turned 'On'. At the bottom, there are 'Save' and 'Cancel' buttons.

I choose to send alerts to admins

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview Policies interface titled 'Create rule'. The page is titled 'Create rule' and includes the sub-instruction 'Allow overrides from Microsoft 365 files and Microsoft Fabric items'. There is a checkbox for 'Allow users to override policy restrictions in Fabric (including Power BI), Exchange, SharePoint, OneDrive, and Teams.' Below this is a section for 'Incident reports' with a 'Severity level' dropdown set to 'High'. A toggle switch 'On' is followed by the instruction 'Send an alert to admins when a rule match occurs.' Below this is a section for 'Send email alerts to these people (optional)' with a 'Add or remove users' button. Two radio button options are shown: 'Send alert every time an activity matches the rule' (selected) and 'Send alert when the volume of matched activities reaches a threshold'. Under the second option, there are fields for 'Instances more than or equal to' (set to 15) and 'Volume more than or equal to' (set to 0 MB). Below these is a field 'During the last' (set to 60 minutes) and 'For' (set to All users). A toggle switch 'On' is followed by the instruction 'Use email incident reports to notify you when a policy match occurs.' Below this is a section for 'Send notifications to these people' with an email address 'argbc2025@argbc2025.onmicrosoft.com' and a 'Add or remove users' button. A note states 'All incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered.' A link 'You can also include the following information in the report:' is present. At the bottom are 'Save' and 'Cancel' buttons.

I make sure action is taken with rule match occurs

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the 'Create policy' wizard in Microsoft Purview. The left sidebar lists steps: 'Template or custom policy' (checked), 'Name' (checked), 'Admin units' (checked), 'Locations' (checked), 'Policy settings' (checked), 'Advanced DLP rules' (unchecked), 'Policy mode' (unchecked), and 'Finish' (unchecked). The main pane is titled 'Customize advanced DLP rules'. It contains a sub-section 'Create rule' with a '+ Create rule' button and a note '3 items'. Below this is a table of existing rules:

Name	Status
Low volume of content detected DLP – UK Financial Info Alert	On
High volume of content detected DLP – UK Financial Info Alert	On
UK Financial DLP - Alert	On

Details for the first rule: Conditions (Content contains any of these sensitive info types: Credit Card Number) and Actions (Restrict access to the content, Send incident reports to Administrator, Send alerts to Administrator, Evaluate rule per component).

At the bottom are 'Back', 'Next', and 'Cancel' buttons.

I review the customised options

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a web browser window titled "Amit - 101572711" displaying the Microsoft Purview Data Loss Prevention "Create policy" interface. The left sidebar lists steps: "Template or custom policy" (checked), "Name" (checked), "Admin units" (checked), "Locations" (checked), "Policy settings" (checked), "Policy mode" (selected), and "Finish". The main content area is titled "Policy mode" and contains the following text: "You can test this policy before turning it on to verify if it needs improvement or if it meets all your objectives. If you turn the policy on right away, you can edit it later and safely test those changes in simulation mode." It includes three radio button options: "Run the policy in simulation mode" (unchecked), "Turn the policy on immediately" (checked), and "Leave the policy turned off" (unchecked). Below these options are two checkboxes: "Show policy tips while in simulation mode" (unchecked) and "Turn the policy on if it's not edited within fifteen days of simulation" (unchecked). At the bottom are "Back", "Next", and "Cancel" buttons.

I turn the policy on

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser interface for creating a DLP policy. On the left, a vertical checklist shows steps completed (checkmarks) and one pending (blue dot). The steps are: Template or custom policy, Name, Admin units, Locations, Policy settings, Policy mode, and Finish. The 'Finish' step is highlighted with a blue circle. The main right panel is titled 'Review and finish'. It contains sections for 'The information to protect' (U.K. Financial Data), 'Name' (DLP – UK Financial Info Alert), 'Description' (Helps detect financial information in United Kingdom), 'Locations' (with a note about Teams and a 'Update locations' button), 'Policy settings' (with options for low and high volume alerts), and 'Turn policy on after it's created?' (set to Yes). At the bottom are 'Back', 'Submit', and 'Cancel' buttons.

I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

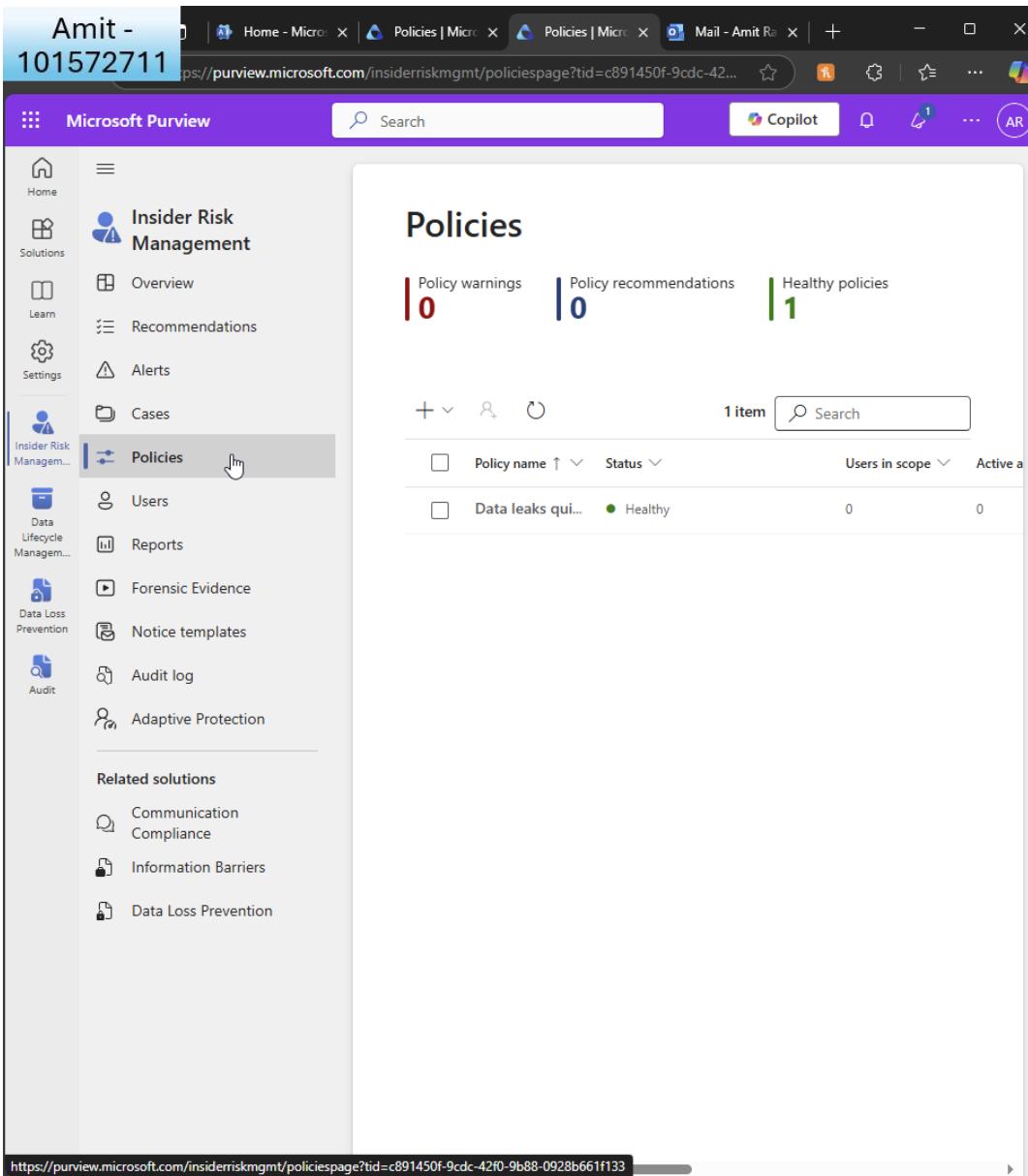
The screenshot shows a Microsoft Purview browser window titled "Amit - 101572711". The URL is https://purview.microsoft.com/datalossprevention/policies?tid=c891450f-9cdc-42f0... The page displays a success message: "New policy created" with a green checkmark icon. It states: "Data loss prevention policy has been created." Below this, under "Next steps", it says: "Monitor alerts to review policy matches. [Learn about reviewing alerts](#)". A "RECOMMENDATION" box contains the text: "You're protecting this sensitive data, now make sure it's deleted when no longer relevant to your organization." It also includes a "Secure Now" button. On the left, a vertical flowchart shows the steps taken: "Template or custom policy" (checkmark), "Name" (checkmark), "Admin units", "Locations", "Policy settings", "Policy mode", and "Finish" (checkmark). At the bottom, there is a "Related tasks" section with three items: "Create an insider risk policy to investigate and take action on insider risks and threats" (with a "Get started" button), "Create a records management policy to automatically retain or delete sensitive content" (with a "Get started" button), and "Create a communication compliance policy to detect inappropriate content in messages" (with a "Learn more" button). A "Done" button is located at the bottom center.

From here I directly go to creating an insider risk policy

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



The screenshot shows the Microsoft Purview Insider Risk Management Policies page. The left sidebar has a 'Policies' section selected. The main area displays policy statistics: 0 Policy warnings, 0 Policy recommendations, and 1 Healthy policies. A table below shows one item: 'Data leaks qui...' status is 'Healthy', with 0 users in scope and 0 active alerts. The URL in the address bar is <https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=c891450f-9cdc-42f0-9b88-0928b661f133>.

I go to 'policies'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview Insider Risk Management interface. On the left, a sidebar lists various management categories like Home, Solutions, Learn, Settings, and several sub-sections under 'Insider Risk Management'. The main panel is titled 'Create a data leak policy' and contains fields for 'Policy name' (set to 'UK Financial DLP Link - Data Leaks') and 'User scope' (set to 'I want to choose specific users and groups'). A dropdown menu shows a user named 'Daniel Singh'. Below these, a section titled 'Settings we filled in for you' lists a triggering event ('User performs an exfiltration activity') and indicators, which include a bulleted list of various SharePoint-related sharing behaviors. At the bottom, there are 'Create policy' and 'Customize' buttons.

I create a data leak policy (quick) create

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Purview Insider Risk Management interface. On the left, there's a navigation sidebar with various options like Home, Solutions, Learn, Settings, and several sub-sections under 'Insider Risk Management'. The 'Policies' section is currently selected. The main content area displays a confirmation message: 'Your data leak policy is being created'. It includes a note about staying up-to-date on the policy and two checkboxes for email notifications: 'Email me when policies have unresolved warnings' (unchecked) and 'Email me when new high severity alerts are generated' (checked). A button labeled 'Update notification settings' is present. Below this, a section titled 'What happens next?' lists four steps: 1. A clock icon: 'It'll take a few minutes to create the policy. You'll see it listed on the Policies tab.' 2. A shield icon: 'Once the policy is active, it could take at least 24 hours for the triggering event to occur and score user activity, at which point the first alert is generated. If admin notification are turned on, you'll get an email when this alert happens.' 3. A gavel icon: 'You or someone on your team will triage the alert and confirm it to a case for further investigation or dismiss it as normal behavior.' 4. A pencil icon: 'After reviewing a few alerts, fine tune your policy to control how many alerts are generated, what activities are detected, and more. We'll provide recommendations along the way.' At the bottom right of the main content area is a 'Done' button.

I see the confirmation

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser window titled "Amit - 101572711". The URL is https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=c891450f-9cdc-42... The page is titled "Edit UK leaks quick policy". On the left, a vertical navigation pane lists steps: "Policy template" (checkmark), "Name and description" (checkmark), "Users and groups" (checkmark), "Content to prioritize" (checkmark), "Triggering event" (highlighted with a blue circle), "Indicators" (radio button), and "Finish" (radio button). The main content area is titled "Choose triggering event for this policy". It explains that users can choose one or more triggering events to determine when a policy begins assigning risk scores. A radio button is selected for "User matches a data loss prevention (DLP) policy". Below it, a dropdown menu shows "DLP – UK Financial Info Alert". Another radio button is available for "User performs an exfiltration activity". A section titled "Select which activities will trigger this policy" contains several checkboxes: "Downloading content from SharePoint" (checked), "Sending email with attachments to recipients outside the organization" (checked), "Printing files" (unchecked), "Creating or copying files to USB" (unchecked), and "Using a browser to upload files to the web" (unchecked). A yellow callout box points to the first checkbox with the text: "① Unable to select some indicators? This is because they're currently turned off in your organization. To make them available to select, you can turn them on now." A "Turn on indicators" button is located next to the callout. At the bottom are "Back", "Next", and "Cancel" buttons.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser window titled "Amit - 101572711". The URL is https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=c891450f-9cdc-42... The page is titled "Edit UK leaks quick policy". On the left, there's a vertical navigation menu with the following steps: Policy template, Name and description, Users and groups, Content to prioritize, Triggering event, **Indicators** (which is the current step), Detection options, Indicator thresholds, and Finish. To the right of the menu, the main content area has a title "Choose threshold type for indicators". It explains that each indicator uses thresholds to influence activity risk scores and determine alert severity. Three options are listed:

- Apply thresholds provided by Microsoft: Built-in thresholds will be applied to all indicators you selected.
- Apply thresholds specific to your users' activity: RECOMMENDED. Thresholds based on users' recent activity patterns will be applied to all built-in indicators you selected.
- Choose your own thresholds: Customize thresholds that are prepopulated with values based on users' recent activity patterns.

At the bottom of the screen are "Back", "Next", and "Cancel" buttons.

I choose default thresholds by MS

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows a Microsoft Purview browser window titled 'Amit - 101572711'. The URL is https://purview.microsoft.com/insiderriskmgmt/policiespage?tid=c891450f-9cdc-42... The page displays a 'Review settings and finish' section for an 'Edit UK leaks quick policy'. On the left, a vertical checklist shows steps completed (Policy template, Name and description, Users and groups, Content to prioritize, Triggering event, Indicators) and one step pending (Finish). The right side details the policy settings: Policy type (Data leaks), Policy name and description (UK leaks quick policy), Users, groups and adaptive scopes (Daniel Singh), Content to prioritize (None), Triggering event (DLP policy: DLP – UK Financial Info Alert), and Policy indicators (34/114 selected, No customized thresholds). Navigation buttons at the bottom include Back, Submit (highlighted in blue), and Cancel.

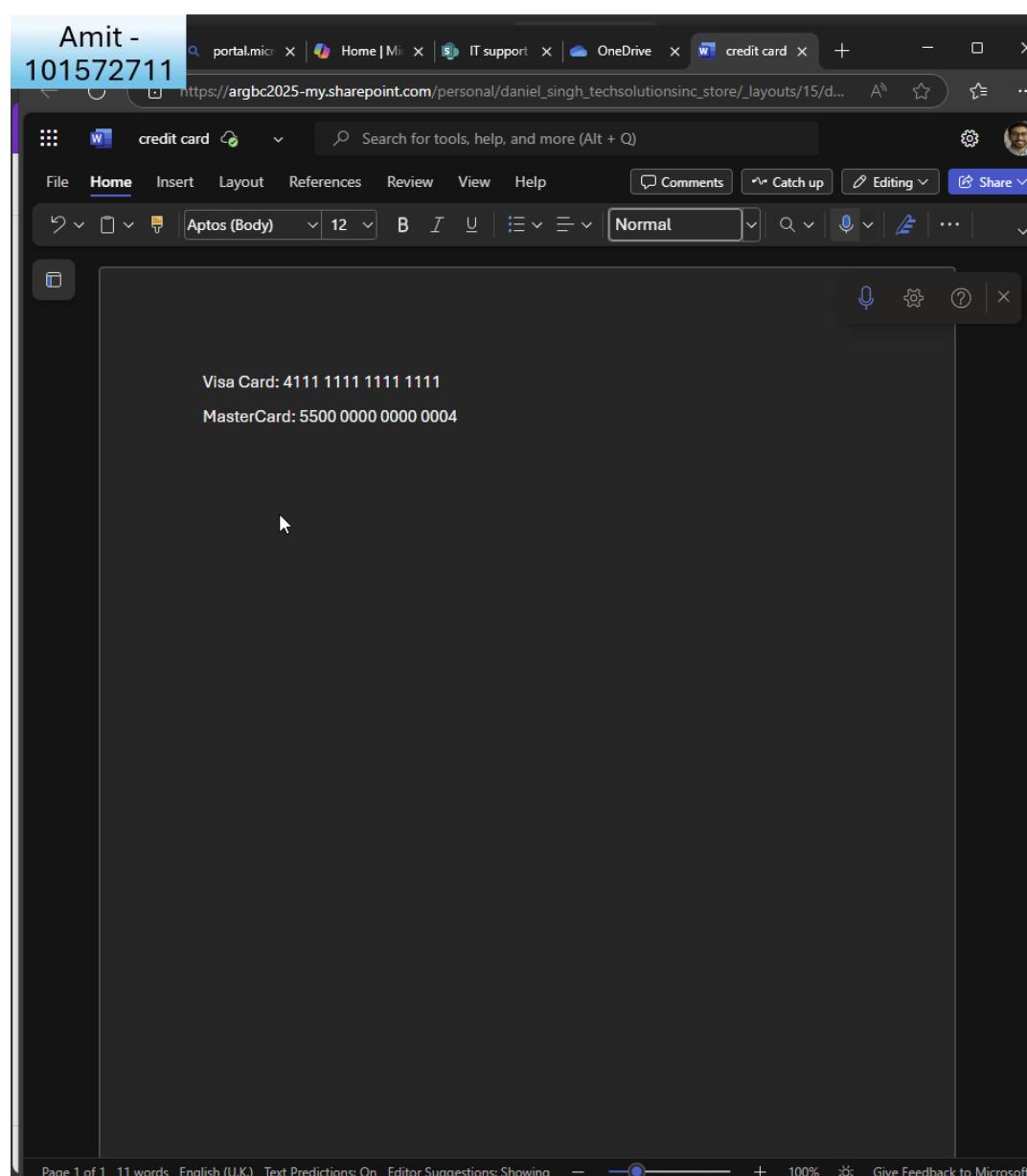
I review and finish

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



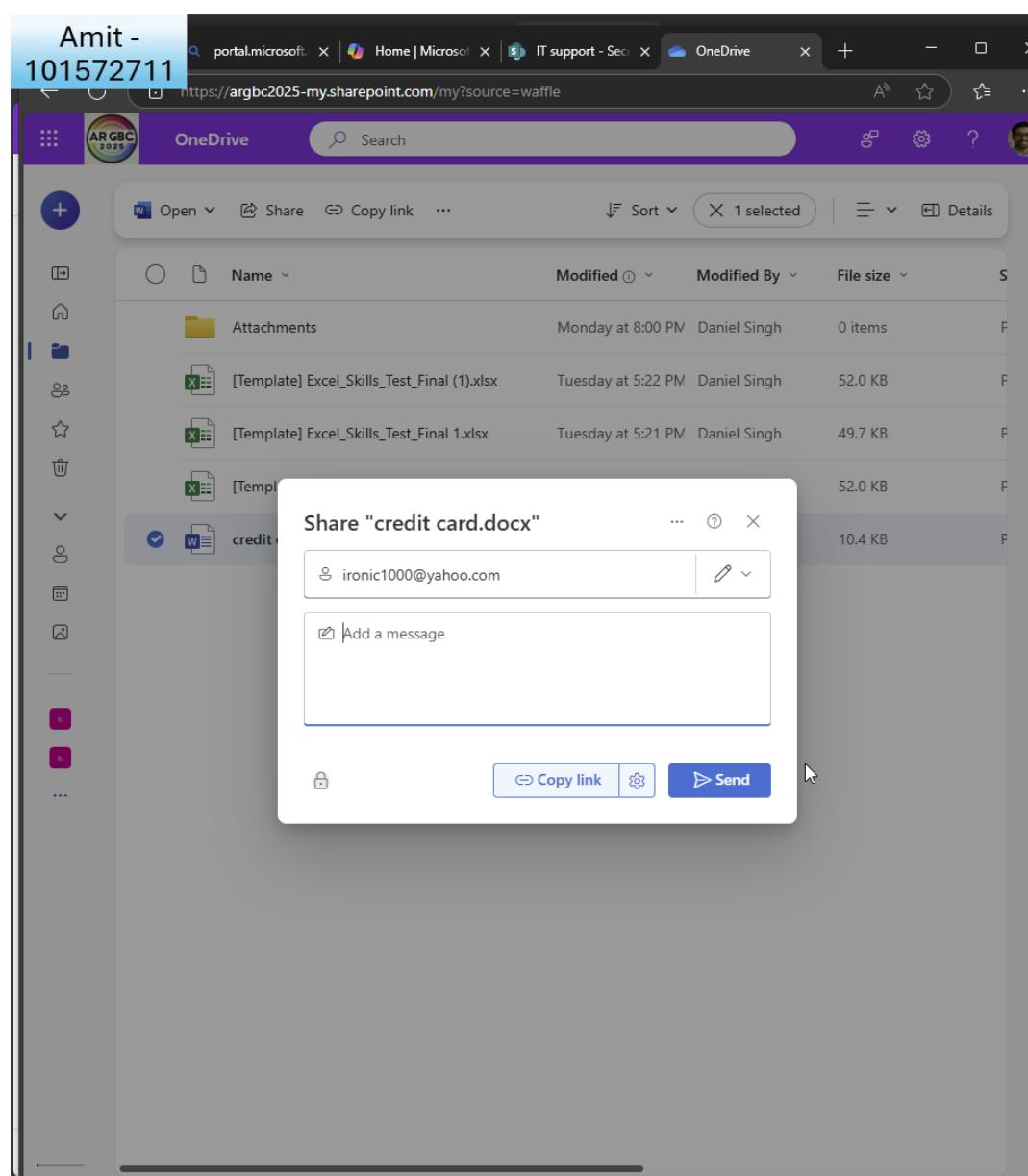
I create a 'dummy' credit card file as user 'Daniel'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I share it externally

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Outlook inbox interface. The left sidebar displays navigation options like Home, View, Help, New email, and various folders including Inbox (11 items), Sent Items, Drafts, and Deleted Items. The main pane shows the 'Inbox' tab with a list of messages. A specific message from 'Office365' is highlighted with a red box, indicating it has been blocked. The subject of the message is 'Access Blocked: credit card'. The message body states: 'This item is protected by a policy...'. To the right of the inbox, a detailed view of this blocked message is shown. It includes the recipient ('Daniel Singh'), date ('Thu 17/04/2025 21:37'), and a note: 'This message is from a trusted sender.' Below this, a warning states: 'This item is protected by a policy in your organization. Access to this item is blocked for everyone except its owner, last modifier, and the site owner. Detected issues from data loss prevention:' followed by a bullet point: 'Item contains the following sensitive information: Credit Card Number'. At the bottom of this panel are 'Reply' and 'Forward' buttons.

I receive a notification as Daniel

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

The screenshot shows the Microsoft Defender interface with the following details:

- Alert Story:** Daniel Singh shared a file "credit card.docx" from an One Drive for Business site.
- Policy matches found in this violation:** Credit Card Number (1 match)
- Policy description:** Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.
- Related events:** Sensitive info found in 'credit card.docx' (Event, User: DANIELSINGH@TEC..., Time detected: Apr 17, 2025 9:37 PM, Location: OneDrive)

And I can see the alert in Defender

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

3. Generate Usage Reports:

- Use the Microsoft 365 admin center to generate reports on user activity, email usage, and SharePoint site usage.

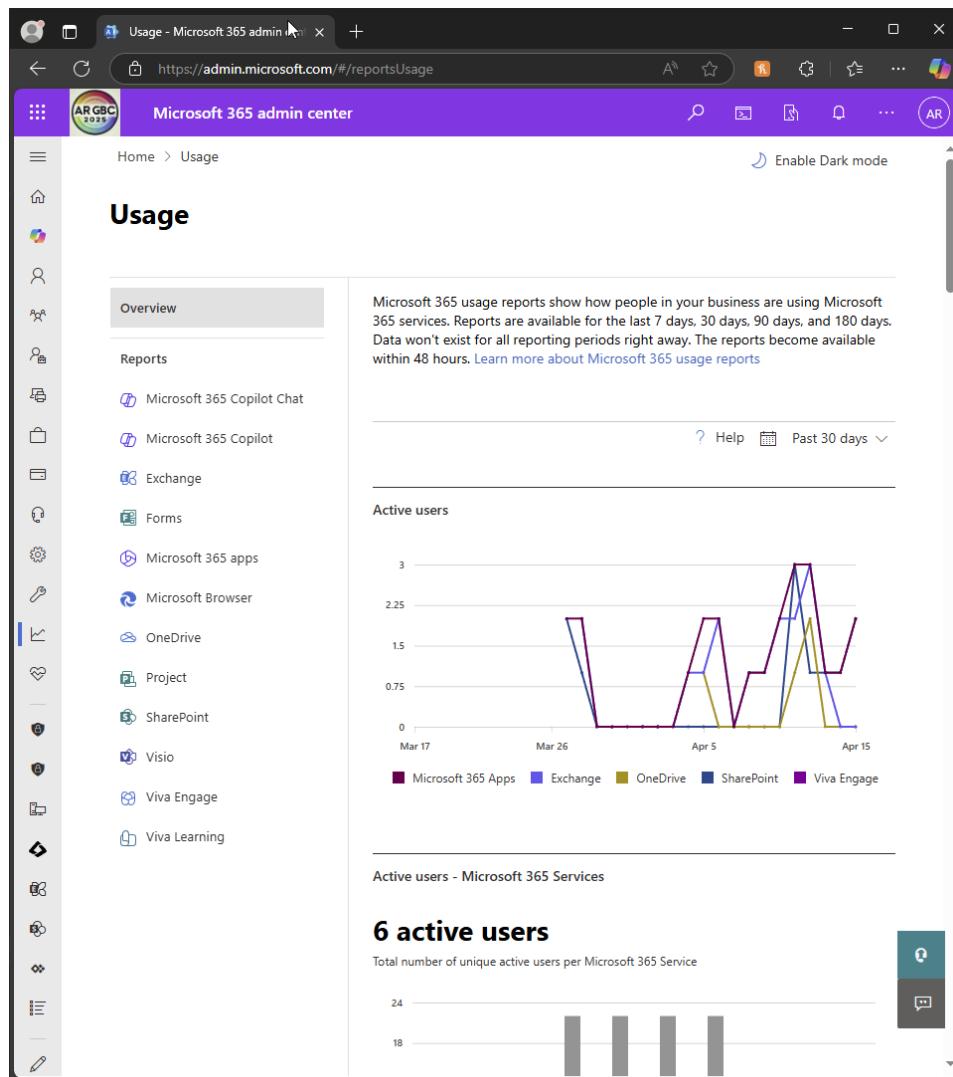
The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a navigation menu with items like Home, Copilot, Users, Groups, Roles, Resources, Marketplace, Billing, Support, Settings, Setup, and Reports. Under Reports, 'Usage' is selected, which is further divided into 'Organizational messages' and 'Health'. The main content area features a banner about syncing Workday data with Microsoft Entra ID and Active Directory. Below the banner is a 'User management' section with buttons for 'Add user', 'Edit a user', 'Reset password', and 'Delete user'. At the bottom, there's a 'Billing' section showing a 'Billing account view' connected to 'ARGBC2025 (MCA)'. The URL in the address bar is <https://admin.microsoft.com/#/reportsUsage>.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

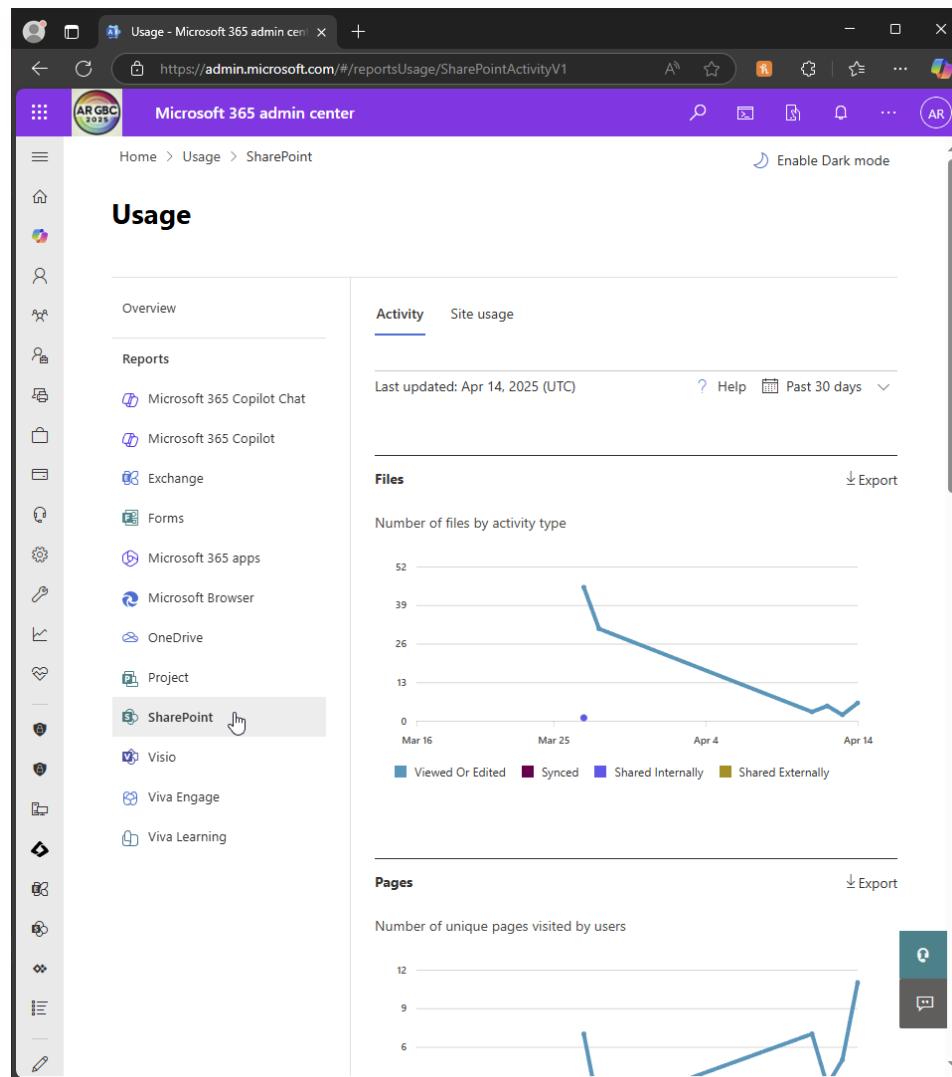


I can see reports such as active users

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

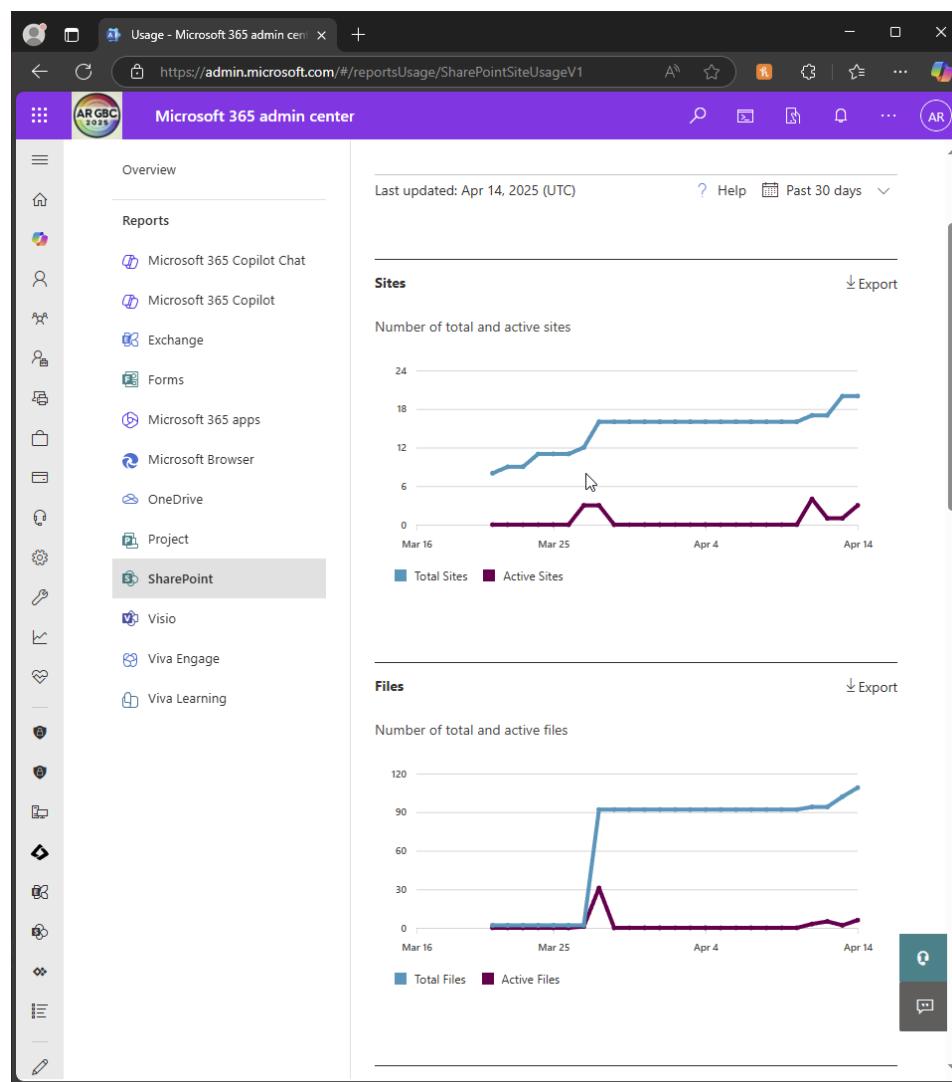


Sharepoint activity i.e. files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



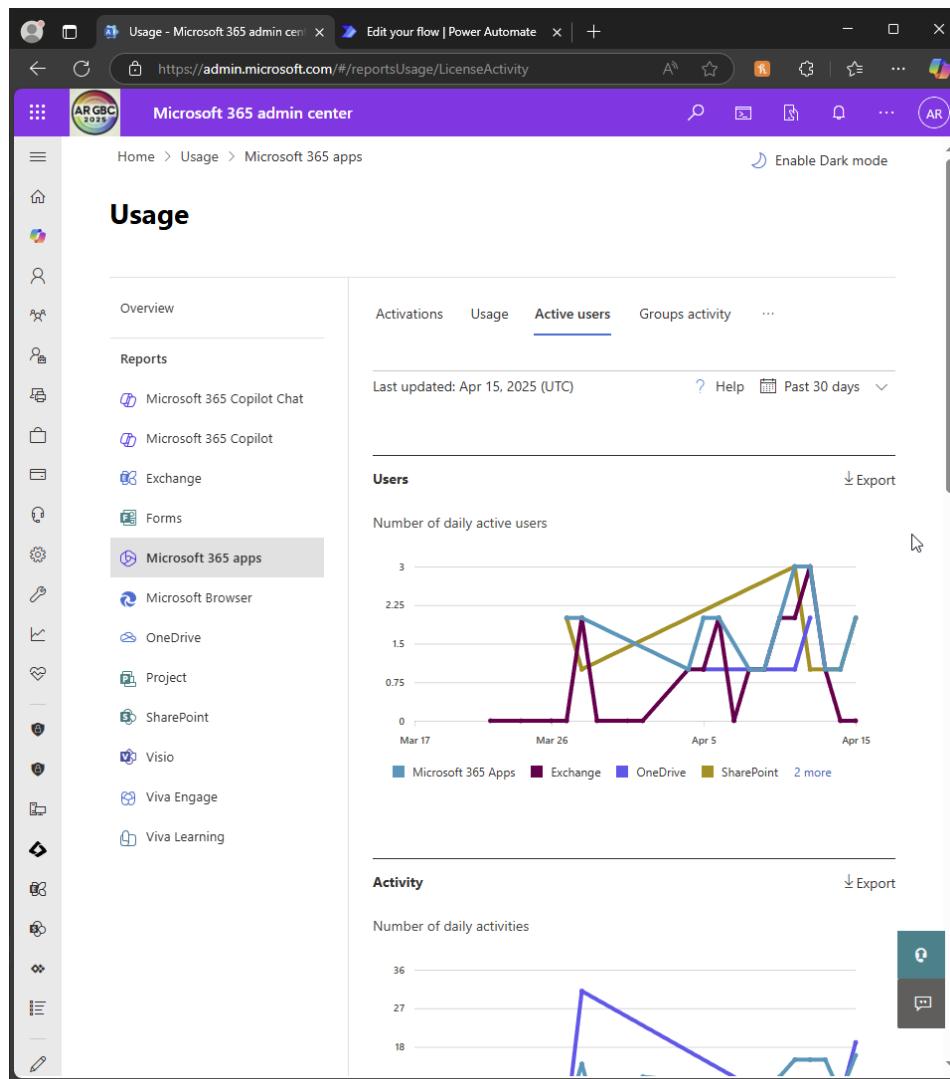
Sharepoint active sites

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

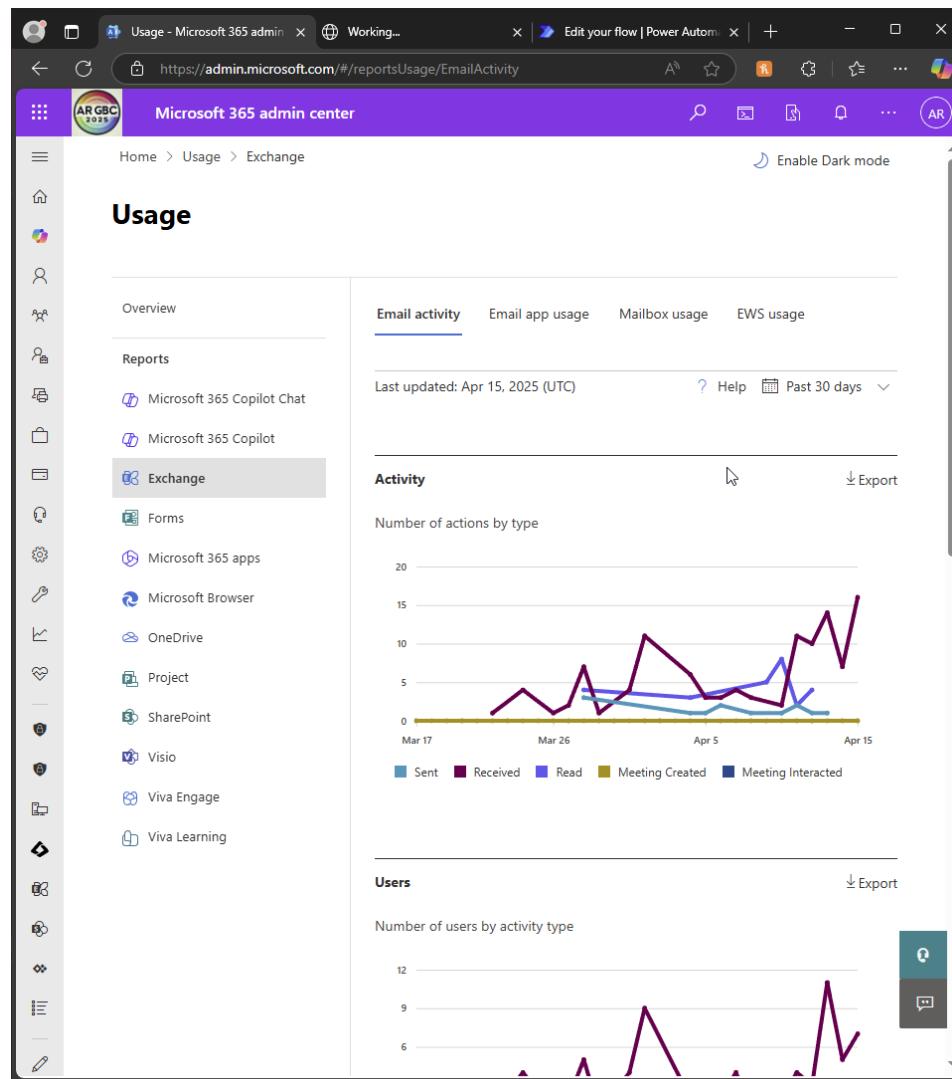


Active users

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

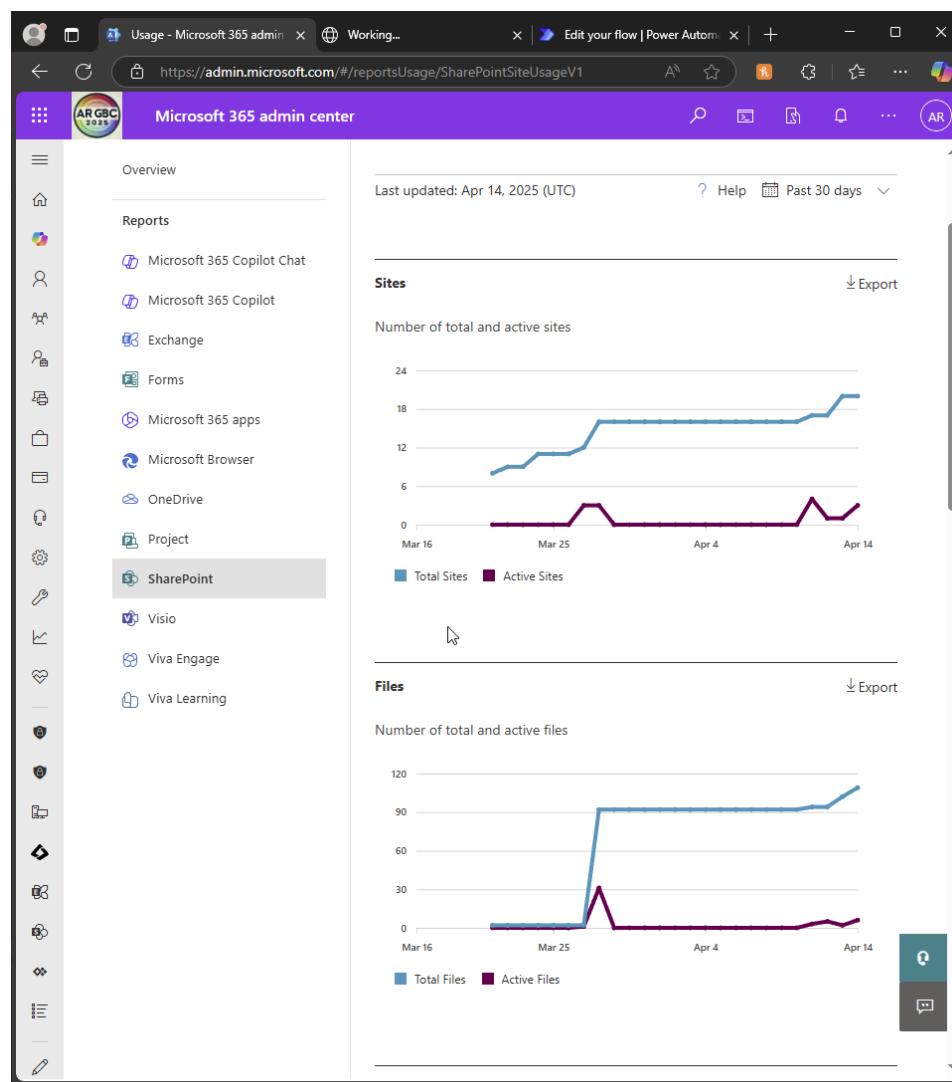


Email activity

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



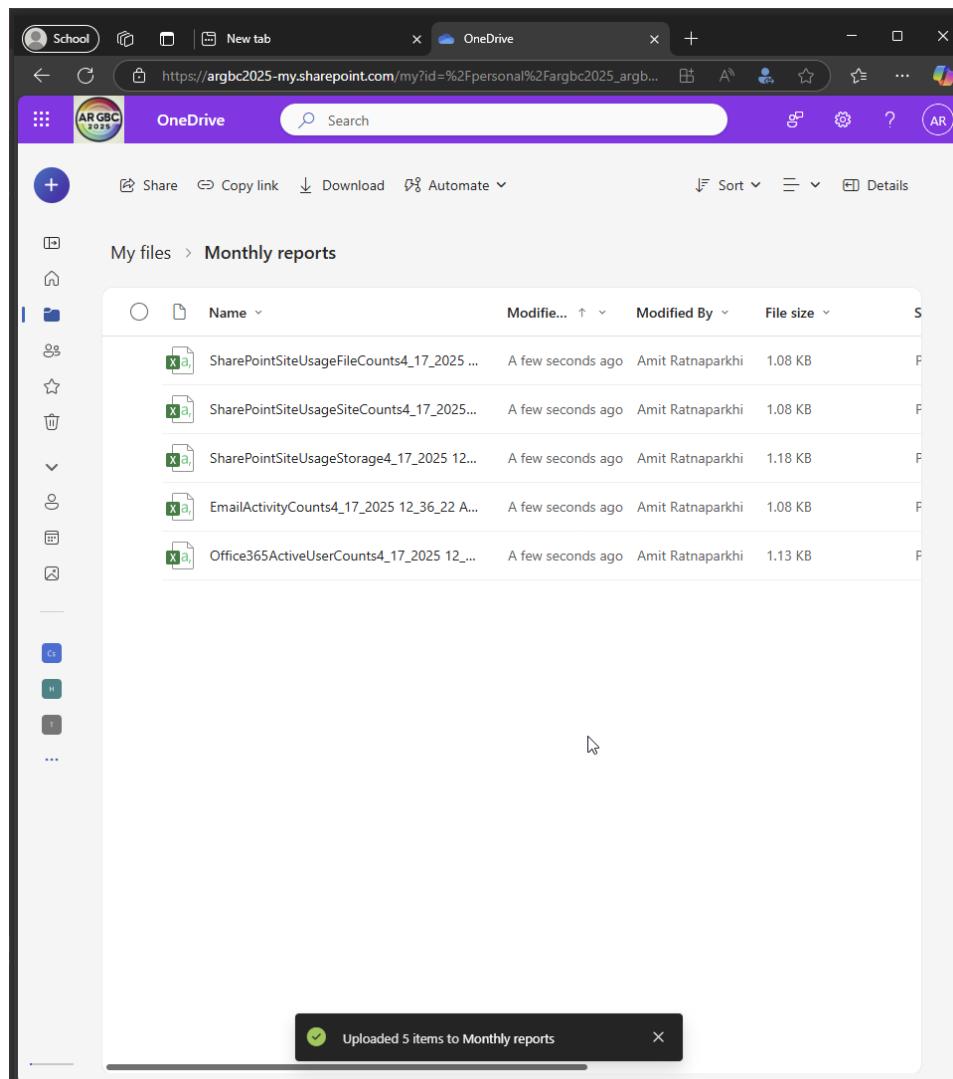
Sharepoint sites and files. Click export to export all of them as CSV files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



I upload them to onedrive 'monthly reports' folder

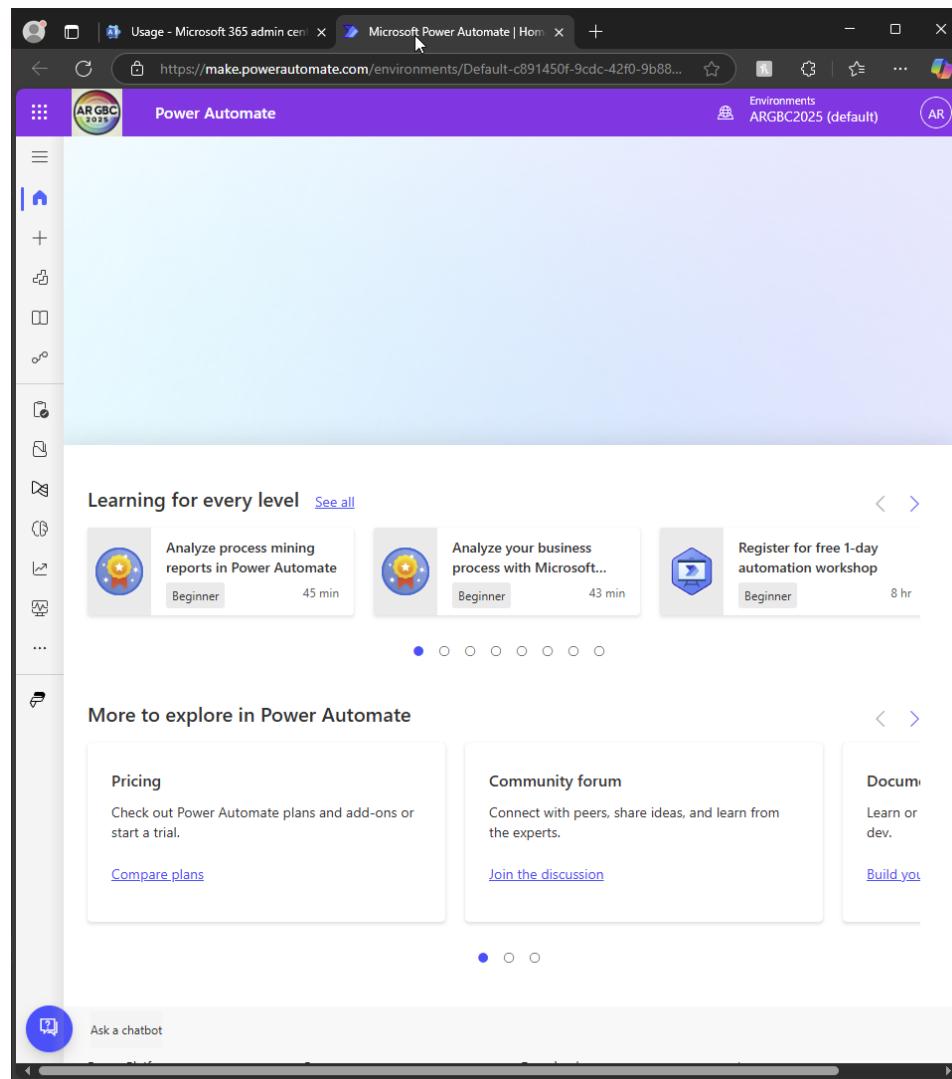
- Schedule monthly reports to be sent to IT administrators and department heads.(Optional, you can use Power Automate)

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



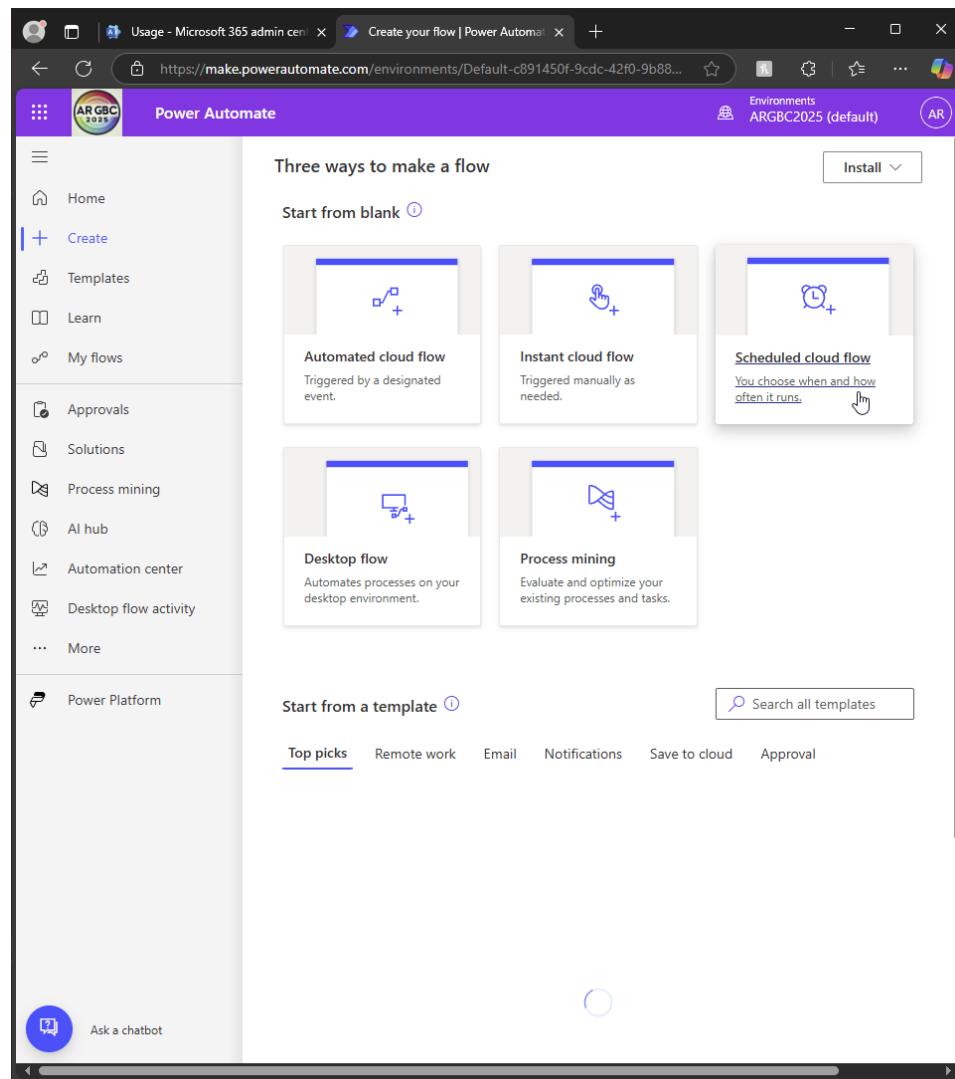
I choose to use Power Automate so I open it up

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

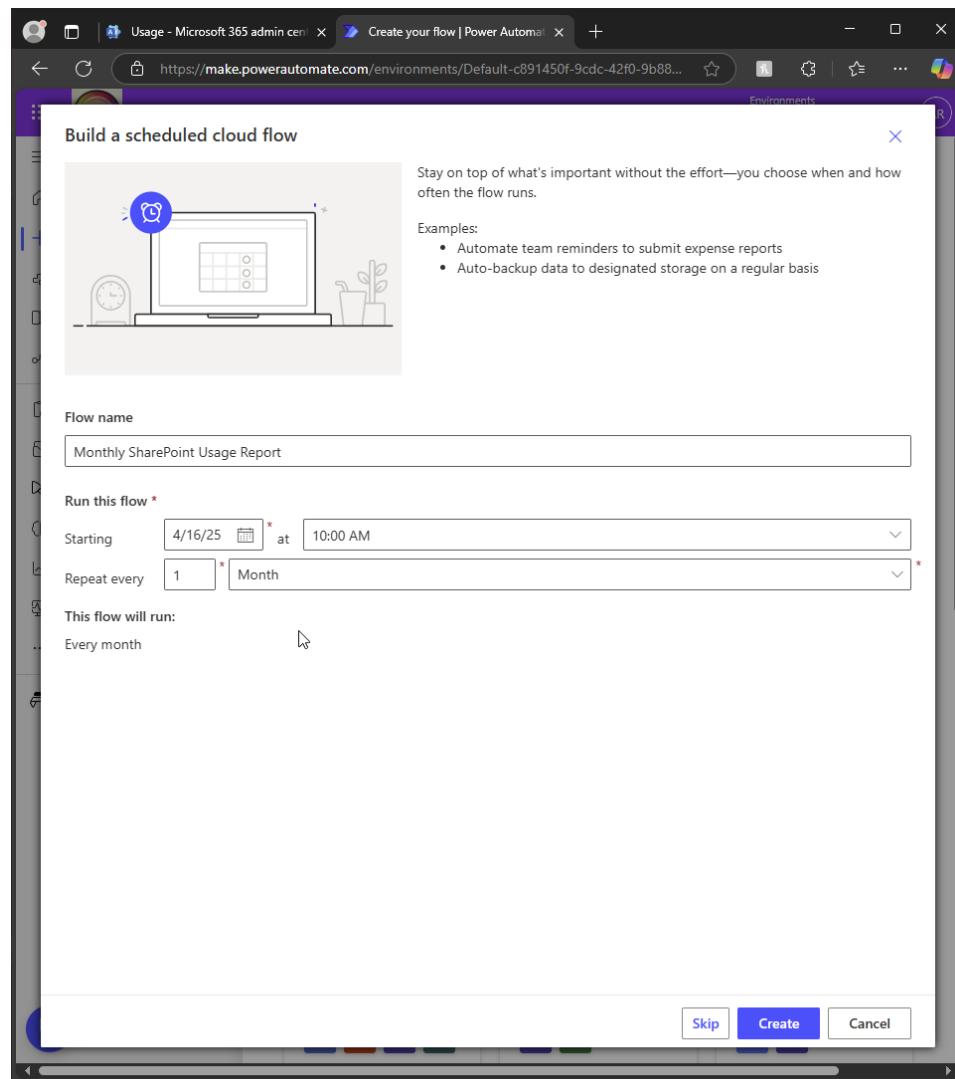


I click 'create'

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



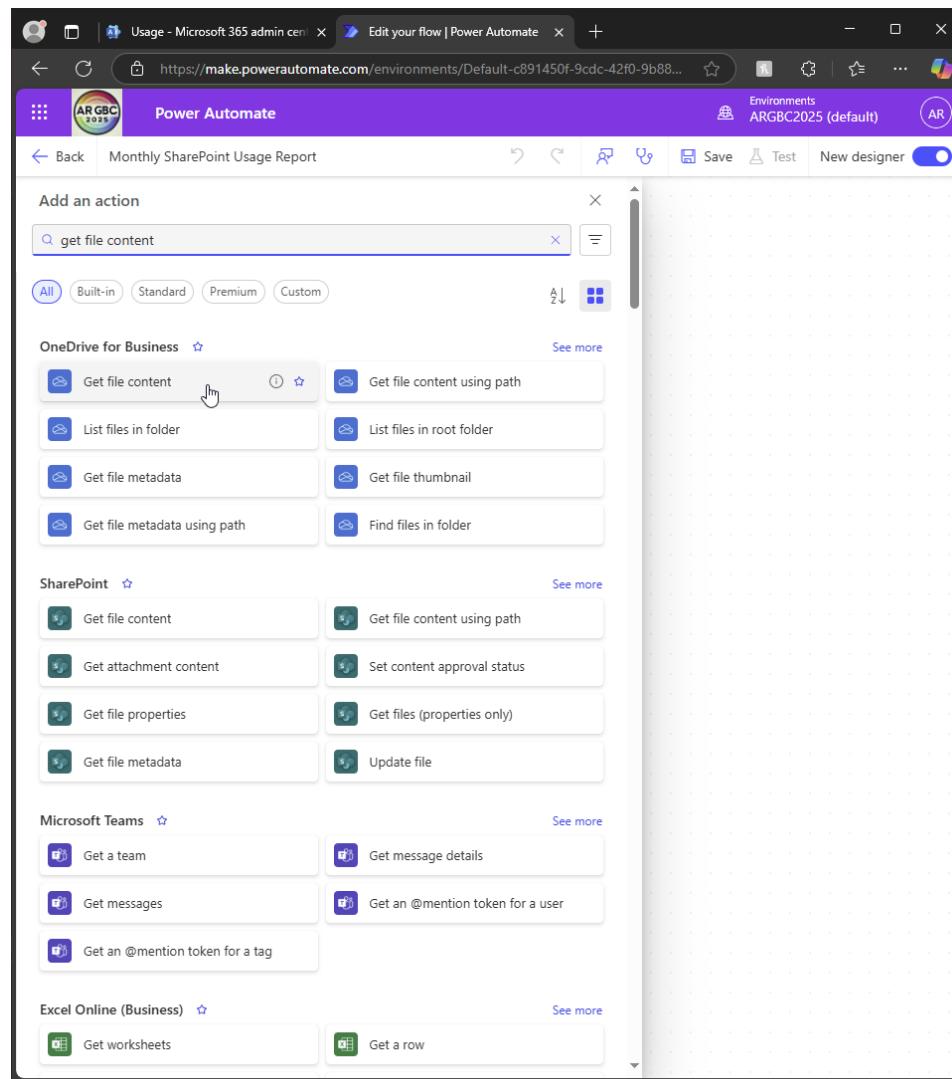
I name my flow and make it monthly

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



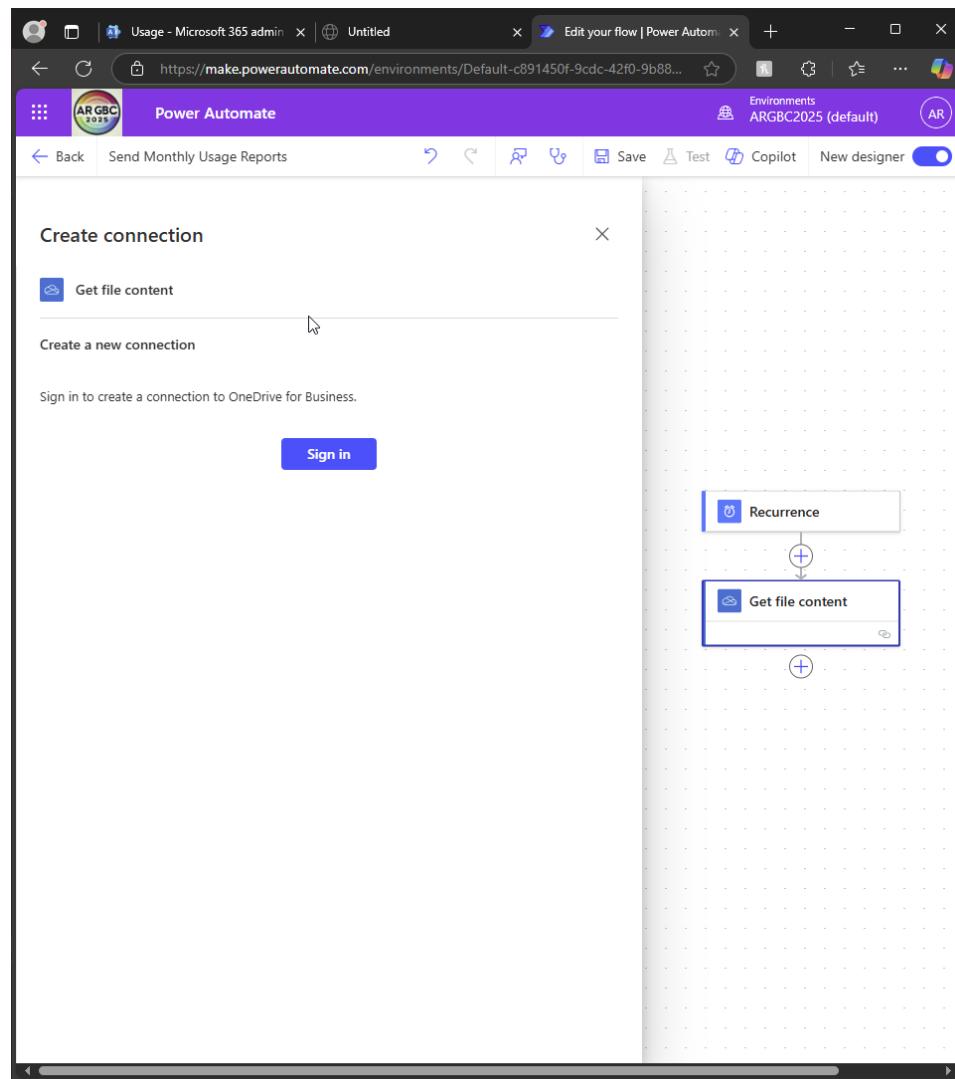
I choose to get file content from onedrive (the place I stored the CSVs)

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



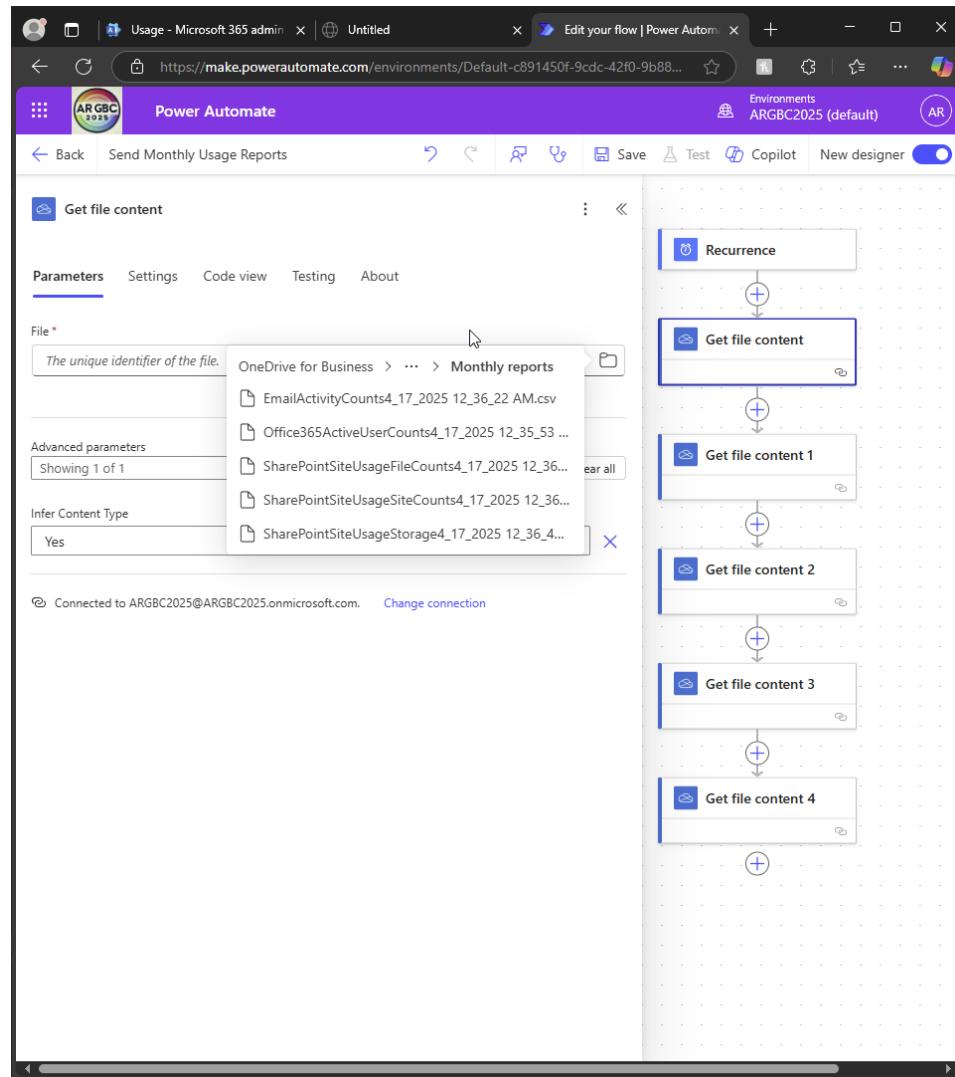
I create the connection with ondrive

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



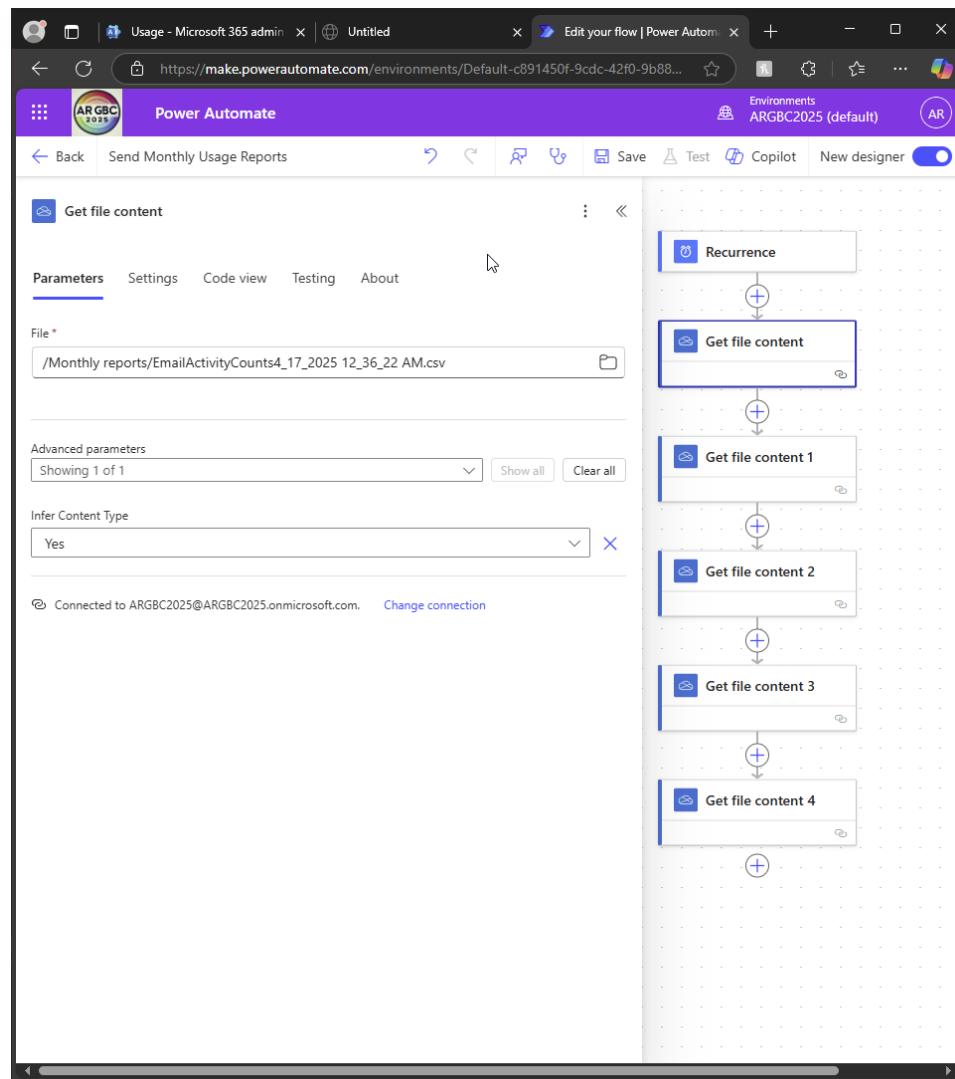
I repeat the process of getting file content so it gets content from all 5 CSV files

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



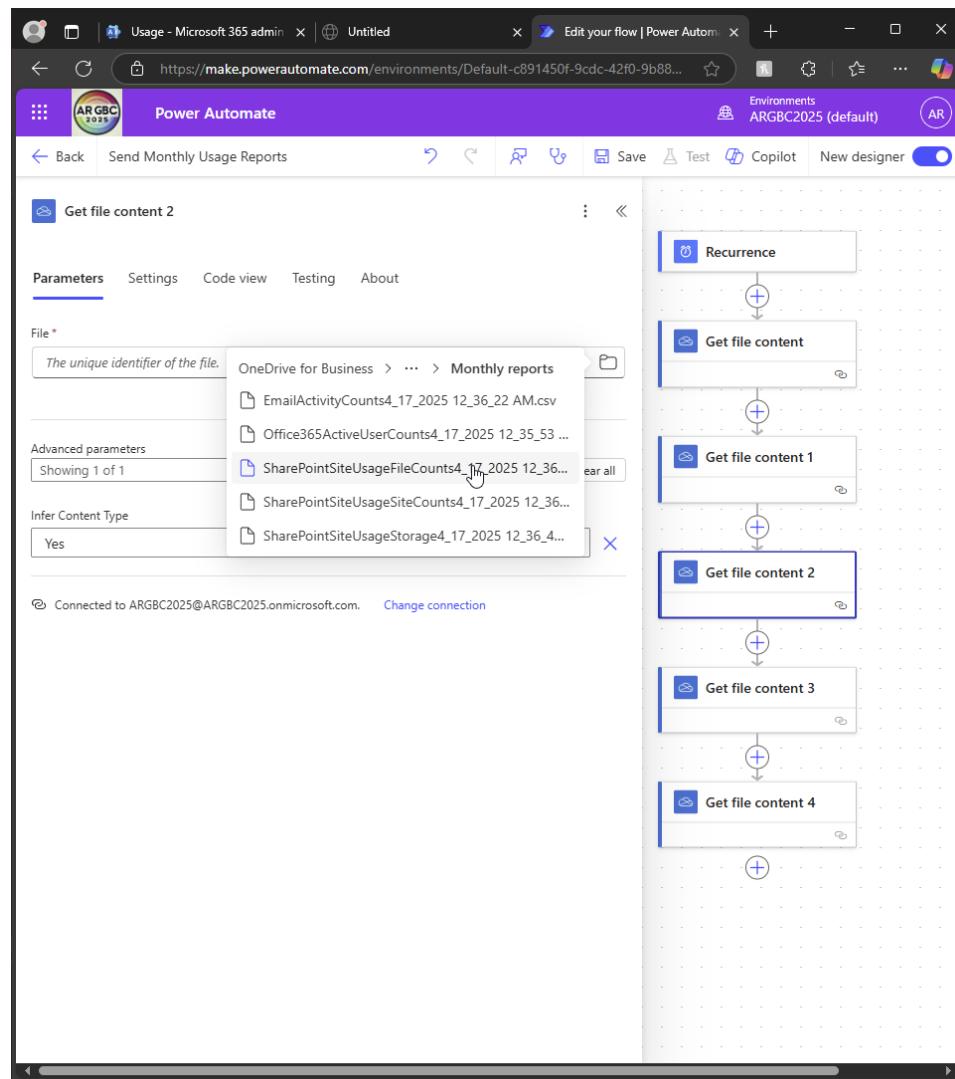
I specify the file

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



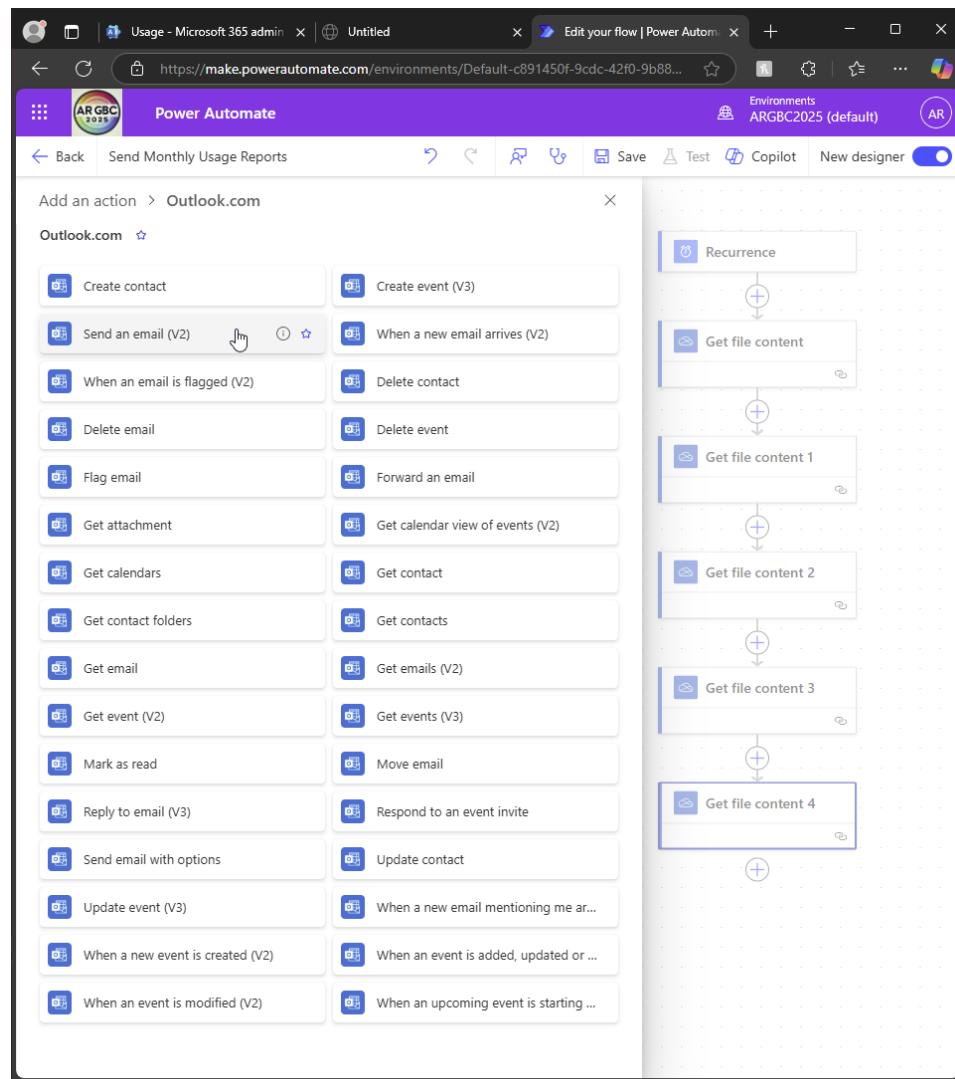
And repeat for each file content flow box

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



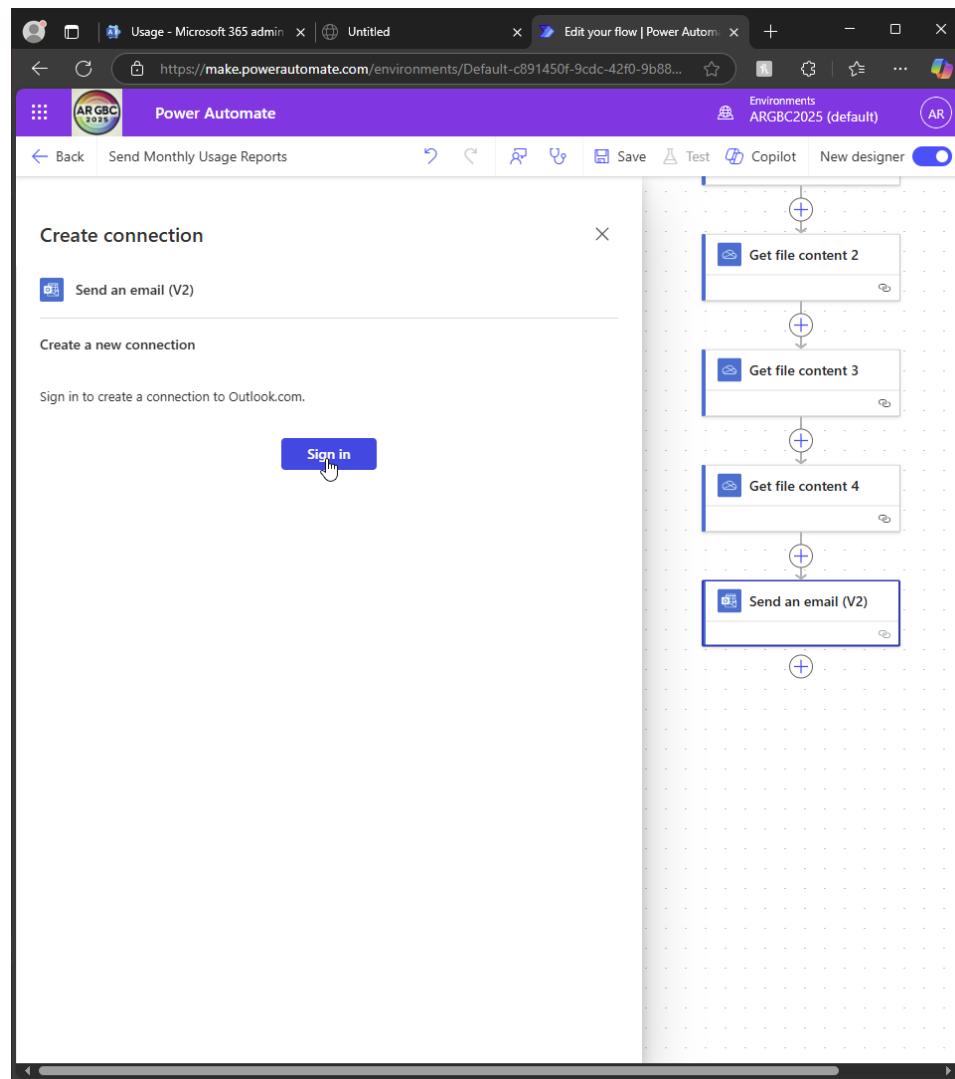
I add an action after 'get file content 4' flow box to send an email

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

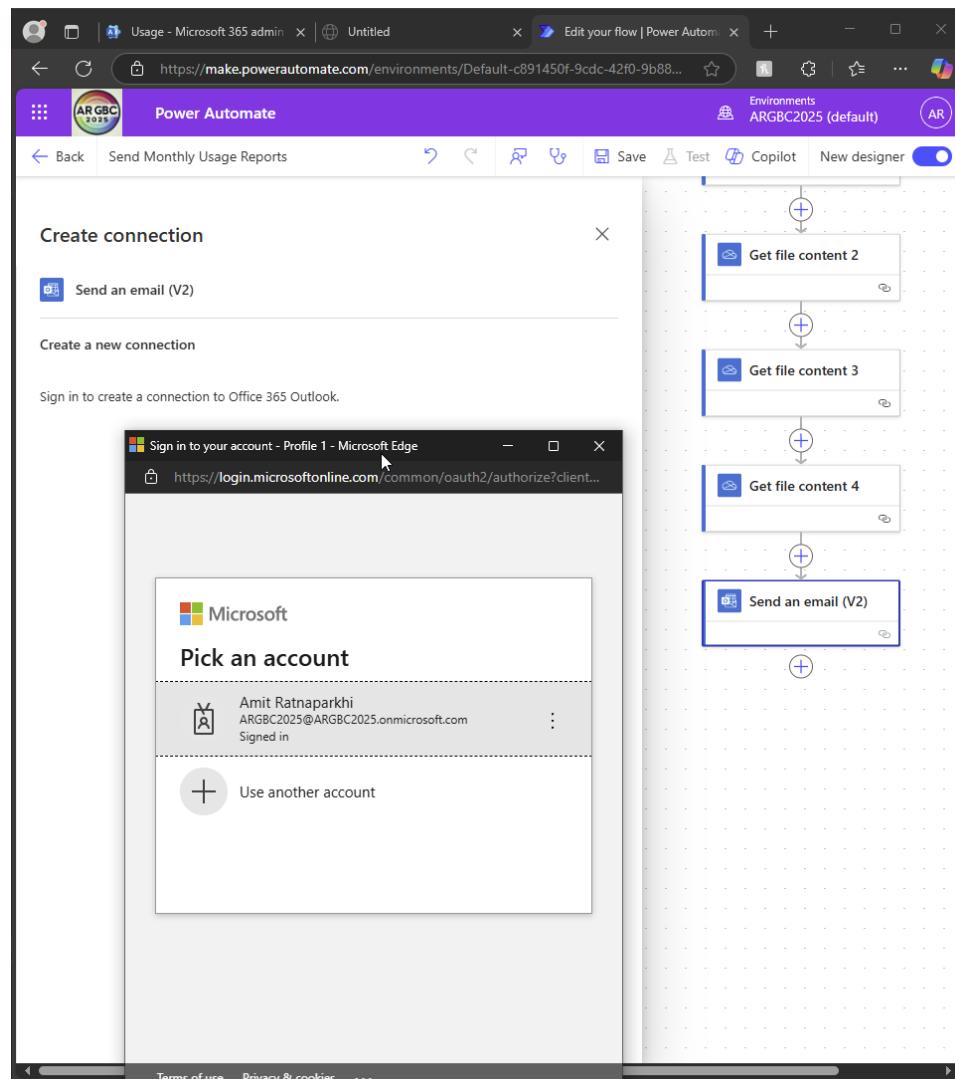


I create the connection to Outlook

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

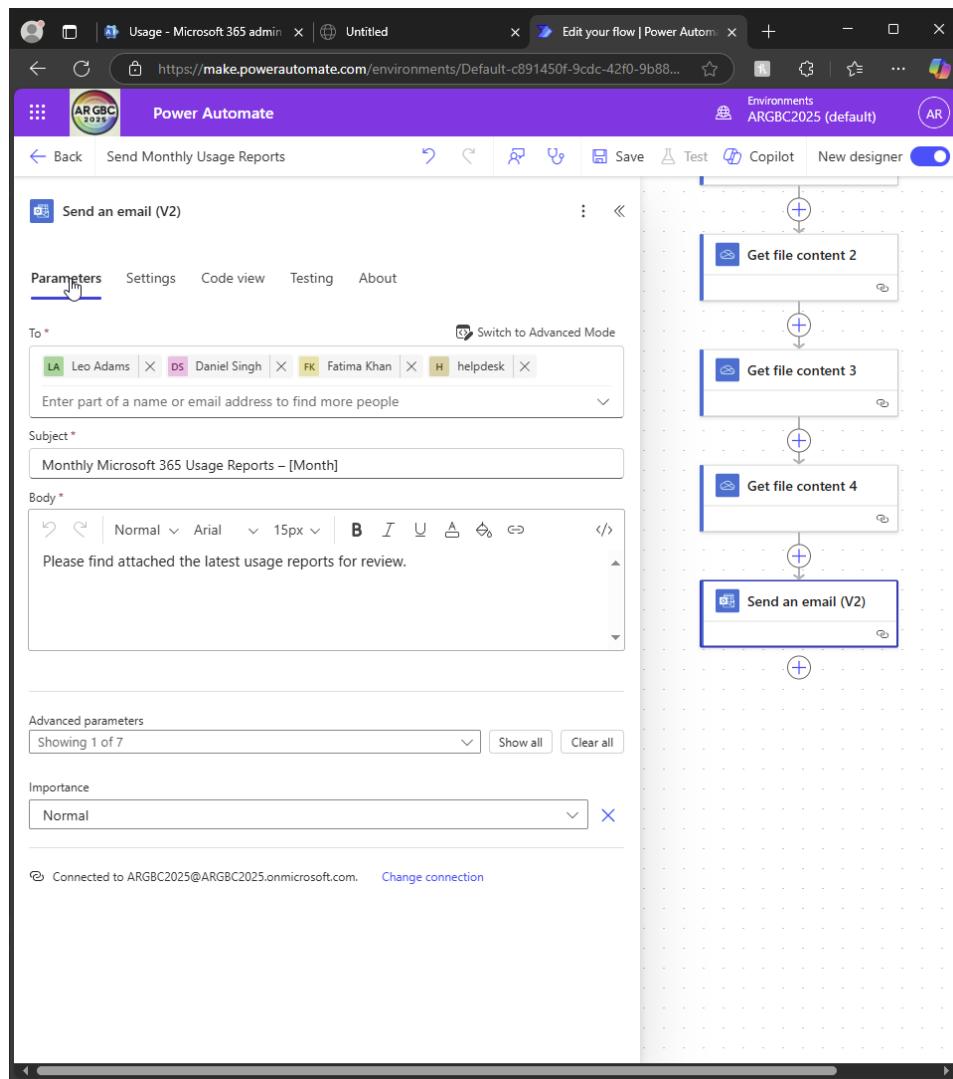


I sign in as GA

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



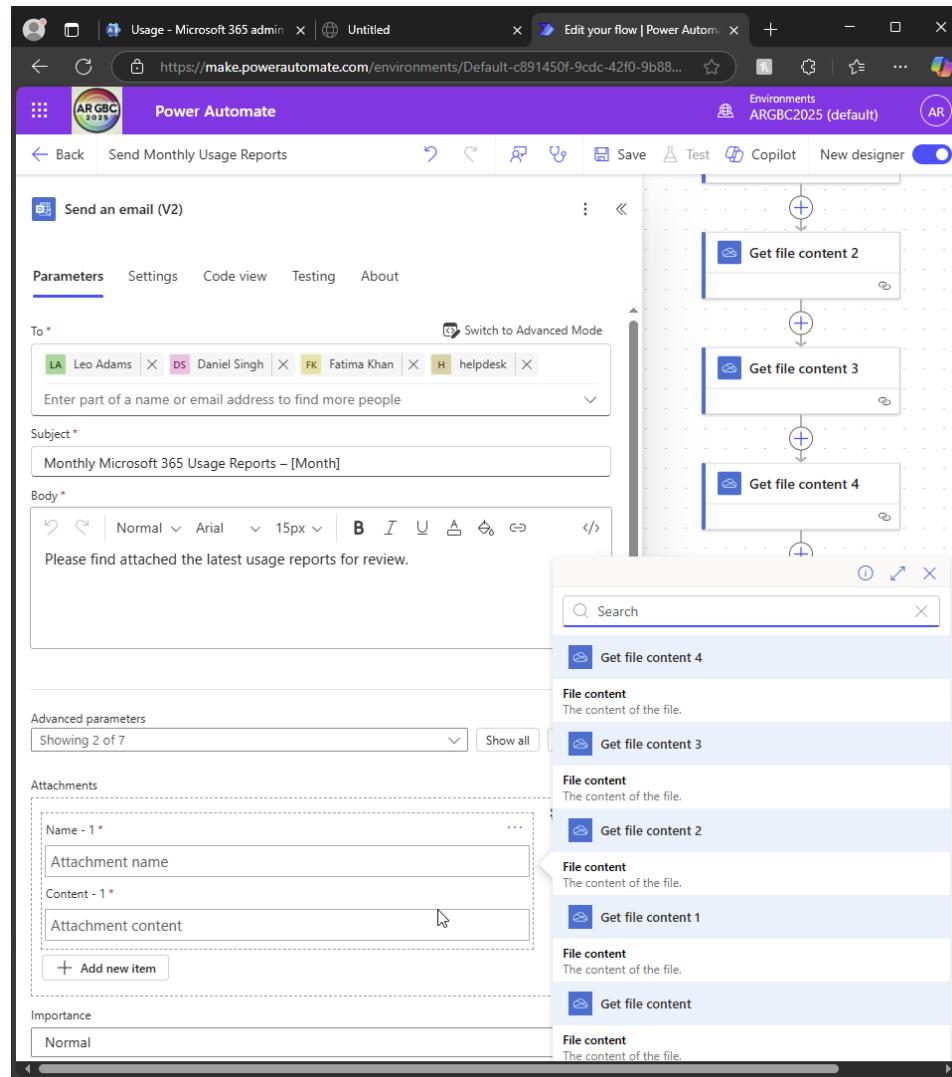
I choose to send the mail to IT departments and department heads

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

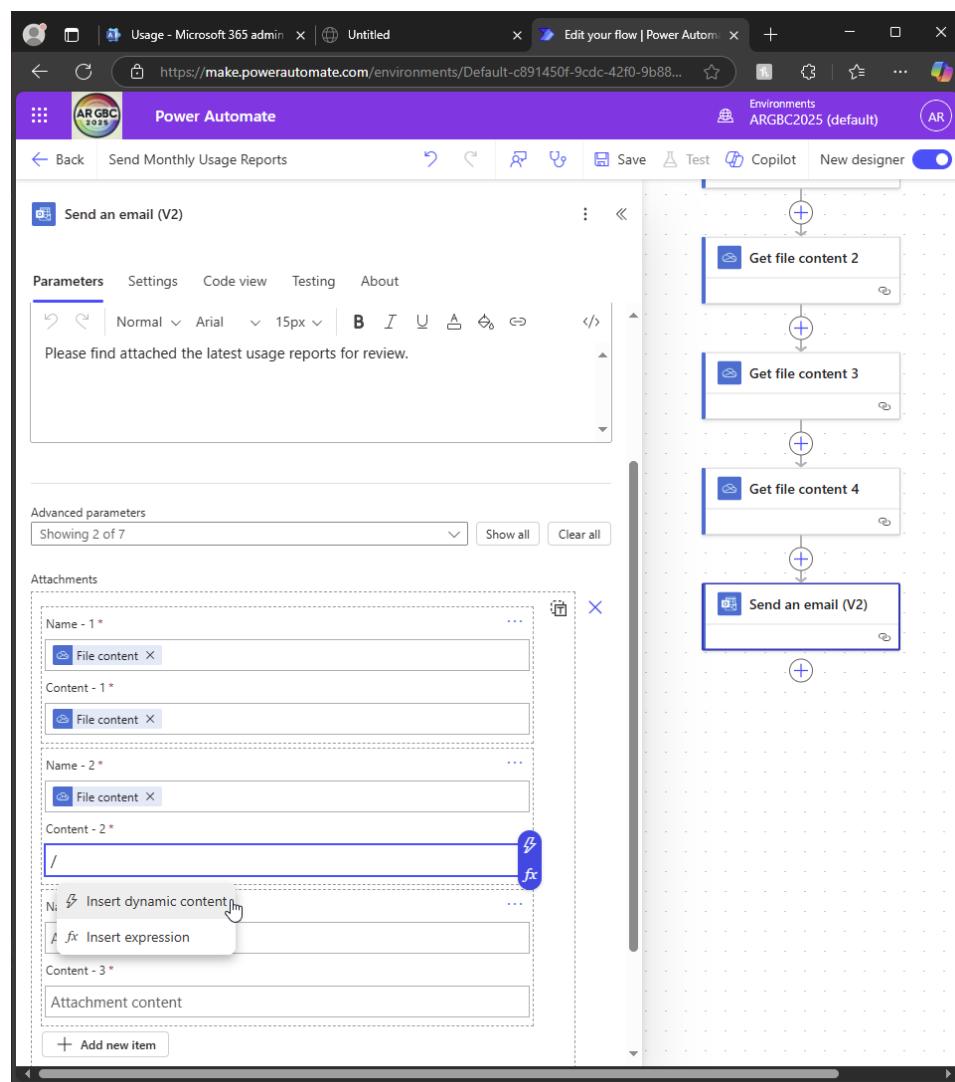


I dynamically attach each file contents

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

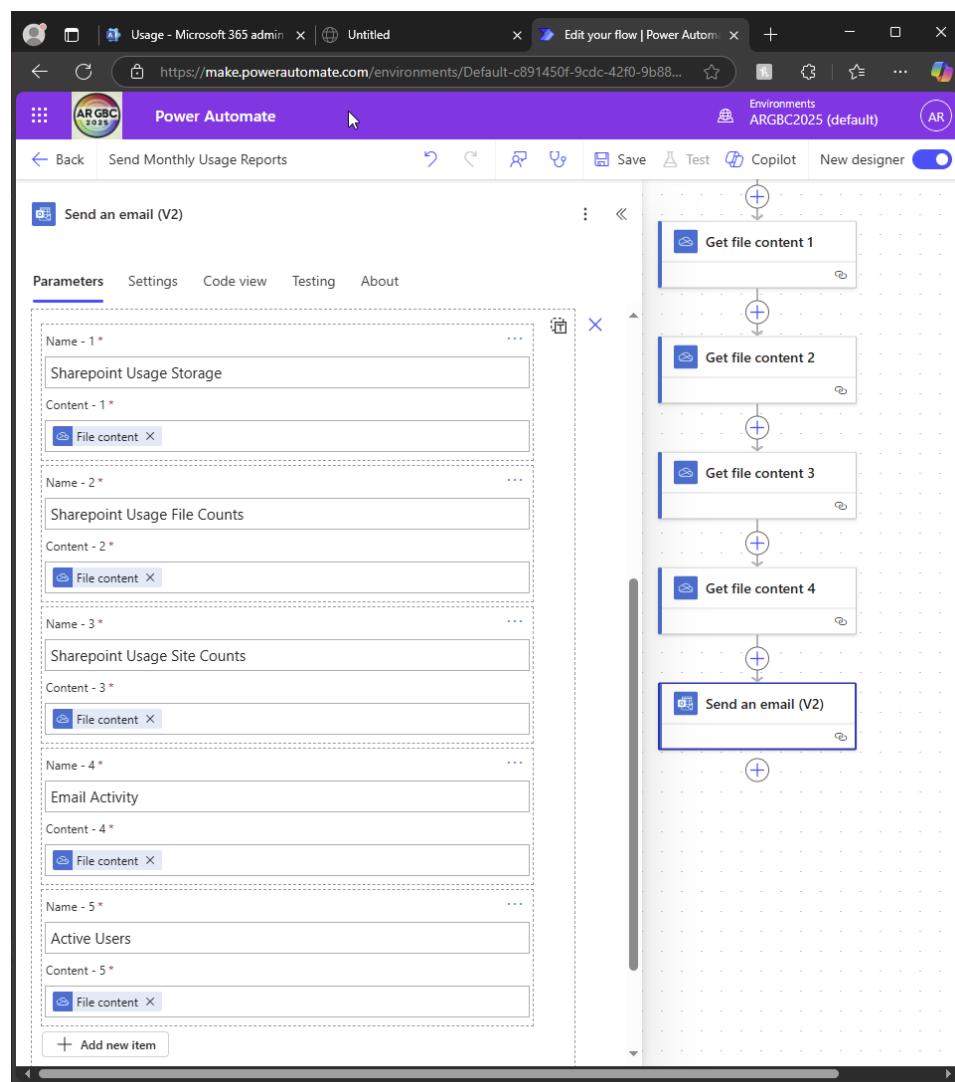


5 times, for each CSV

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

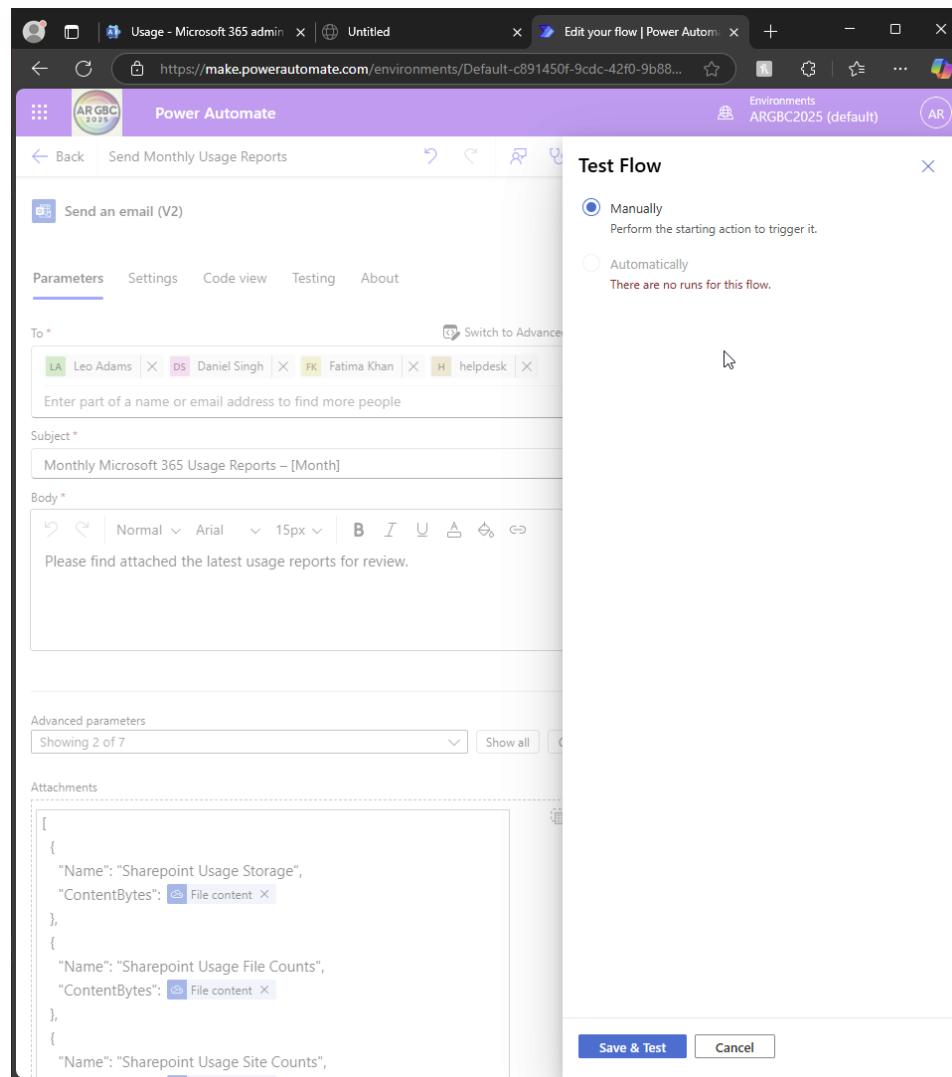


I give meaningful names to each file

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:



I save it and test flow

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows a Microsoft Power Automate interface. At the top, there's a navigation bar with tabs like 'Usage - Microsoft', 'Untitled', 'Edit your flow | Pow...', and 'Manage your flows'. Below the navigation is a purple header bar with the 'Power Automate' logo and the environment name 'ARGBC2025 (default)'. The main area is titled 'Send Monthly Usage Reports > Run history'. It displays a table with one row. The columns are 'Start time', 'Duration', '+ Add column', and 'Status'. The first row shows 'Apr 16, 09:11 PM (19 sec ago)', '00:00:02', '+ Add column', and 'Test succeeded' (which is highlighted with a green background). On the left side, there's a vertical toolbar with various icons for managing flows. At the bottom, there's a blue button labeled 'Ask a chatbot'.

Start time	Duration	+ Add column	Status
Apr 16, 09:11 PM (19 sec ago)	00:00:02		Test succeeded

I confirm the test succeeded

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:
Student ID:

Term:

4. Implement and Monitor Service Health:

- Set up service health alerts to notify administrators of any issues with Microsoft 365 services.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with various links like Resources, Marketplace, Billing, Support, Settings, Setup, Reports, Adoption Score, Usage, Organizational messages, and Health. Under the Health section, 'Service health' is selected, showing options for Windows release health, Message center, Product feedback, Network connectivity, and Software updates. The main content area has a banner for 'Keep user data in sync with Workday data'. Below it, there's a 'User management' section with buttons for Add user, Edit a user, Reset password, and Delete user. At the bottom, there's a 'Billing' section showing a billing account view connected to 'ARGBC2025'.

I go to admin centre - health - service health

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 Admin Center Service Health page. At the top, there's a navigation bar with icons for Home, Service health, and other admin center sections. The main title is "Service health". Below it, there are three tabs: "Overview" (which is selected), "Issue history", and "Reported issues". A sub-header says "View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)". There are two buttons at the top right: "Report an issue" and "Customize". To the right of the "Report an issue" button is a "Change view" icon. The main content area is titled "Active issues Microsoft is working on" and lists several items:

Issue title	Issue type
Users may see an error and can't attach Microsoft 365 data to email messages using the new Outlook for Windows	Advisory
Some users may see an unexpected status for submissions in Microsoft Defender for Office 365	Advisory
Some users' devices may be offered a Windows 11 upgrade despite Microsoft Intune policies being configured otherwise	Advisory
Admins may be unable to run the Get-FederationInformation PowerShell cmdlet in Exchange Online	Advisory
Admins may be unable to validate connectors from the Exchange admin center	Advisory
Users' SharePoint Online pages may be failing to generate thumbnails of webparts	Advisory
Users may see a new "Content Freshness" template option when creating pages in SharePoint Online	Advisory

Below this, there's a section titled "Service status" which shows "Exchange Online" with a status of "3 advisories". On the far right, there are two small teal-colored buttons with white icons.

I check the dashboard

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 admin center interface with the URL <https://admin.microsoft.com/#/servicehealth/:shdpreferences>. The left sidebar has a purple header 'ARGBC 2025' and includes icons for Home, Service health, Overview, Issue history, Reported issues, Report an issue, and Customize. The main content area is titled 'Service health' and shows 'Active issues Microsoft is working on'. It lists several issues such as 'Users may see an error and can't attach files to messages in Outlook on the web or Windows', 'Some users may see an unexpected status message when opening attachments in Microsoft Word', 'Some users' devices may be offered a Windows update that they can't accept', 'Admins may be unable to run the Get-Office365UsagePowerShell cmdlet', 'Admins may be unable to validate connections to Microsoft 365 services', 'Users' SharePoint Online pages may be slow to load', and 'Users may see a new "Content Freshness" metric in the Microsoft 365 Admin Center'. Below this is a section titled 'Service status' which lists 'Service' and 'Exchange Online'. To the right, under 'Customize', there are tabs for 'Page view' (selected) and 'Email'. Under 'Email', there is a section for 'Send me email notifications about service health' with checkboxes for 'Primary email address (ARGBC2025@ARGBC2025.onmicrosoft.com)' and 'Other email addresses'. There are also sections for 'Include these issue types' (Incidents, Advisories, Issues in your environment that require action), 'Include these services' (Dynamics 365 Apps, Exchange Online, Microsoft 365 apps, Microsoft 365 for the web, Microsoft 365 suite, Microsoft Bookings, Microsoft Clipchamp, Microsoft Defender XDR, Microsoft Entra, Microsoft Forms, Microsoft Intune), and a 'Save' button at the bottom.

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

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a sidebar with various icons and sections like Overview, Issue history, and Reported issues. The main area is titled 'Service health' and displays 'Active issues Microsoft is working on'. There are several listed items, each with a brief description. Below this is a section for 'Service status' showing 'Service' and 'Exchange Online'. On the right, a 'Customize' panel is open under the 'Email' tab. It includes fields for 'Primary email address' (set to 'ARGBC2025@ARGBC2025.onmicrosoft.com') and 'Other email addresses' (with a text input field containing 'daniel.singh@techsolutionsinc.store'). There are also sections for 'Include these issue types' (Incidents, Advisories, Issues in your environment that require action) and 'Include these services' (Dynamics 365 Apps, Exchange Online, Microsoft 365 apps, Microsoft 365 for the web, Microsoft 365 suite, Microsoft Bookings, Microsoft Clipchamp, Microsoft Defender XDR, Microsoft Entra). A 'Save' button is at the bottom of the panel.

I ensure GA and IT head are recipients of the email

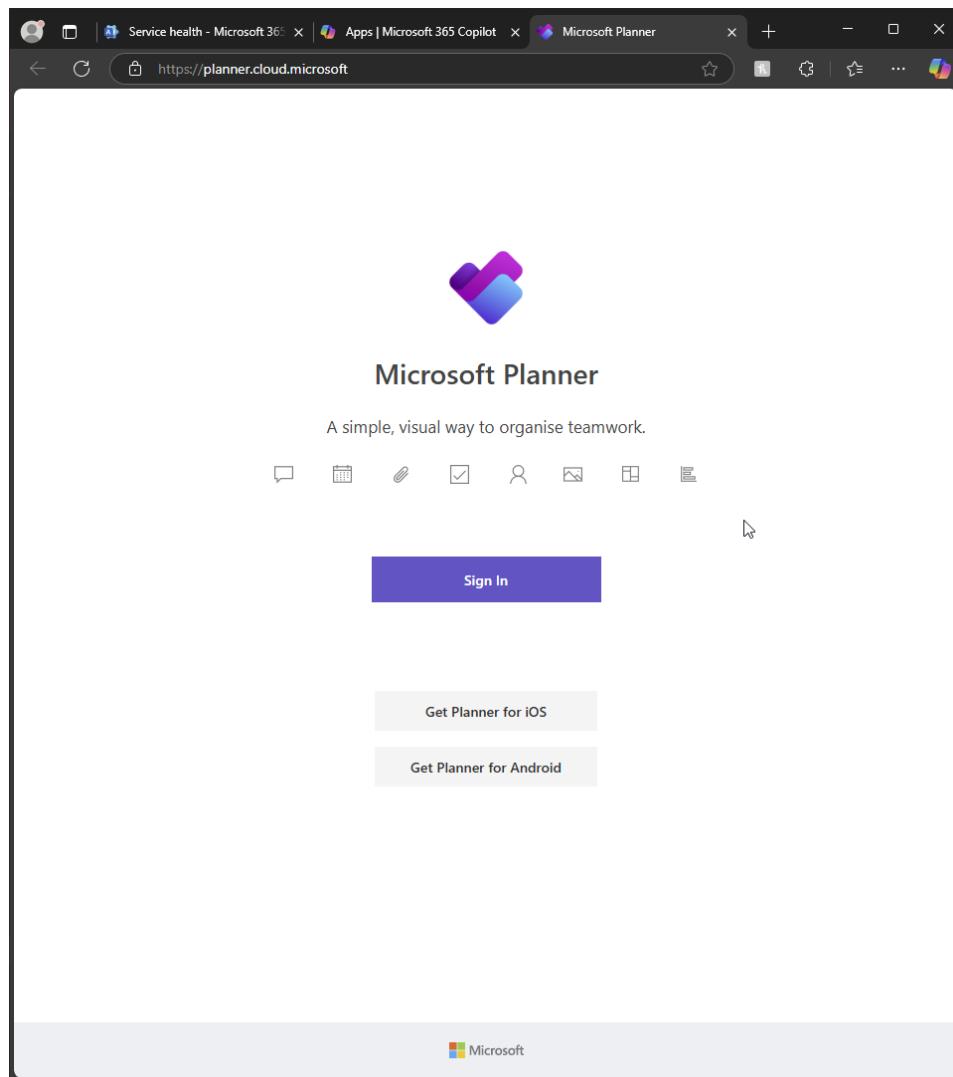
- Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



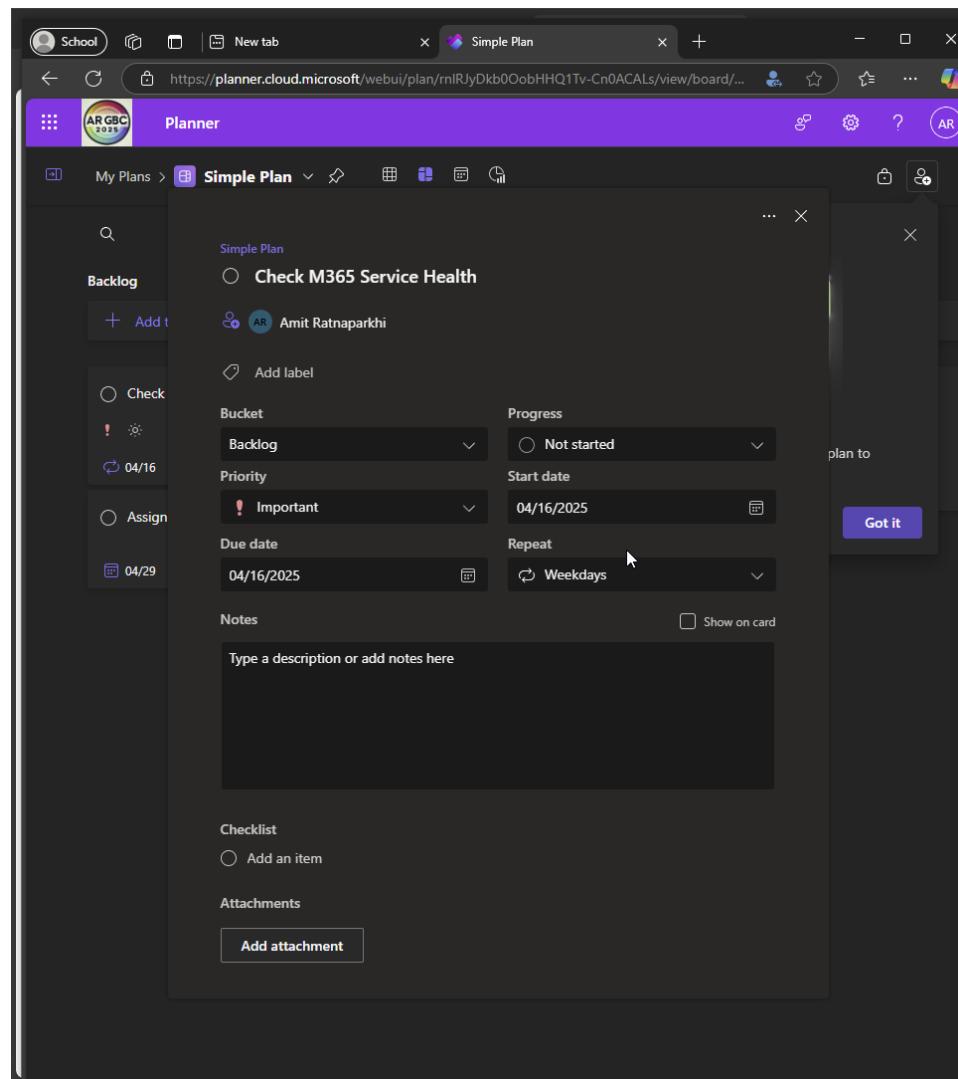
I open MS Planner

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:



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

Microsoft 365 Identity and Services – Enterprise Administration

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 separate 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.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name:

Term:

Student ID:

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 (hurray!) 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.

Microsoft 365 Identity and Services – Enterprise Administration

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