

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

Lab Activity 2: Managing Microsoft 365 Compliance and Security

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

Tasks:

1. Set Up Data Loss Prevention (DLP) Policies

- Access the Microsoft 365 compliance center.
- Create a new DLP policy to protect sensitive information (e.g., credit card numbers).
- Configure the policy to notify users when sensitive information is detected.
- Test the policy by attempting to send an email containing sensitive information.

2. Implement Retention Policies

- Navigate to the Data life cycle management section in the compliance center.
- Create a new retention policy for emails and documents.
- Apply the policy to a specific group of users.
- Verify the policy is working by checking the retention status of emails and documents.

3. Configure and Monitor Security Alerts

- Access the Security center (MS Defender)
- Set up security alerts (Medium severity) if the users created a mail forward/ redirect rule.
- Configure alert notifications to be sent to an administrator.
- Simulate suspicious activity and verify that an alert is triggered.

4. Review and Manage Audit Logs

- Enable auditing in the Microsoft 365 compliance center.
- Search the audit log for specific activities (e.g., file deletions).
- Export audit log data for further analysis.
- Review the exported data to identify any unusual activities.

Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~  
Paste your screenshots here

STARTS ON NEXT PAGE

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

#### 1.1: Access the Microsoft 365 Compliance Center

A: Navigate to Microsoft 365 Admin Center Homepage

The screenshot shows the Microsoft 365 Admin Center interface. At the top, there's a red header bar with the title "Microsoft 365 admin center". Below it, a sidebar on the left lists various administrative tasks: Home, Copilot, Users, Groups, Roles, Resources, Marketplace, Billing, Support, Settings, Setup, Reports, and Health. A user profile card for "Worlanyo Akpatsa" (Student Number 101590287) is displayed. The main content area features a greeting "Good evening, Worlanyo Akpatsa" and a section titled "For organizations like yours" with a "Set up email with a custom domain" card. Below this, there's a "Your organization" section with links for "Users", "Products", "Upcoming changes (5)", "Learn", "Settings", "Help & support", and "Give Feedback". At the bottom, there are buttons for "Add user", "Reset password", "Assign phone number", and a search bar.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with a red box highlighting the user information: "Worlanyo Akpatsa" and "Student Number 101590287". Below this, under "Admin centers", the "Compliance" option is selected, indicated by a blue icon and a small blue arrow. Other options in the sidebar include "Setup", "Reports", "Health", "Security", "Microsoft Intune", "Identity", "Exchange", "SharePoint", "Power Platform", and "All admin centers". At the bottom of the sidebar, there is a link to "Customize navigation". The main content area features a greeting "Good evening, Worlanyo Akpatsa" and a message about the simplified view. It also includes sections for "For organizations like yours" (with a "Set up email with a custom domain" card) and "Your organization" (with tabs for "Users", "Products", "Upcoming changes (5)", "Learn", "Settings", "Help & support", and "Give Feedback"). At the very bottom, there is a footer with links for "Add user", "Reset password", "Assign phone number", and a search bar.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Microsoft Purview Compliance Portal Welcome and Homepage

The screenshot shows a browser window for the Microsoft Purview Compliance Portal. At the top, there's a navigation bar with links like Home, Solutions, Learn, and Settings. A sidebar on the left displays the user information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area features a large blue cloud icon with various service icons (Microsoft 365, Microsoft Azure, AWS, Amazon Web Services, Snowflake, Other cloud platforms & apps) floating around it. Below the icon, a message reads: "Welcome to the new Microsoft Purview portal! and compliance solutions to help you quickly discover and protect data stored across platforms and apps including Microsoft 365, Microsoft Azure, Amazon Web Services, Snowflake, and more. Learn more [?]" There are two comparison tables:

|                 | Protect sensitive info across your data estate | Unified governance & compliance solutions | Upgraded, modern experience |
|-----------------|------------------------------------------------|-------------------------------------------|-----------------------------|
| New portal      | ✓                                              | ✓                                         | ✓                           |
| Classic portals | Limited support                                | Split between separate portals*           | Classic look and feel       |

\*Microsoft Purview compliance portal and Microsoft Purview governance portal

At the bottom, there are "Get started" and "Go to classic portal" buttons.

The screenshot shows the Microsoft Purview Compliance Portal homepage. The layout is similar to the welcome screen, with the same sidebar and user information. The main title is "Purview portal". A central message states: "Microsoft Purview brings together solutions across data governance, data security, and compliance so that you can govern and secure your data wherever it lives." Below this, a section titled "Supported cloud platforms:" lists "Microsoft 365", "Microsoft Azure", "Microsoft Fabric", and "Other cloud platforms". A note at the bottom of this section says: "Having trouble finding specific features or solutions? Some features and solutions from the classic portals either have a new home or were retired. To find the ones that moved, try searching for them above. Review list of relocated and retired features [?]" At the bottom, there are four cards: "Data Catalog", "Information Protection", "Data Loss Prevention", and "View all solutions →".

## Microsoft 365 Identity and Services – Enterprise Administration

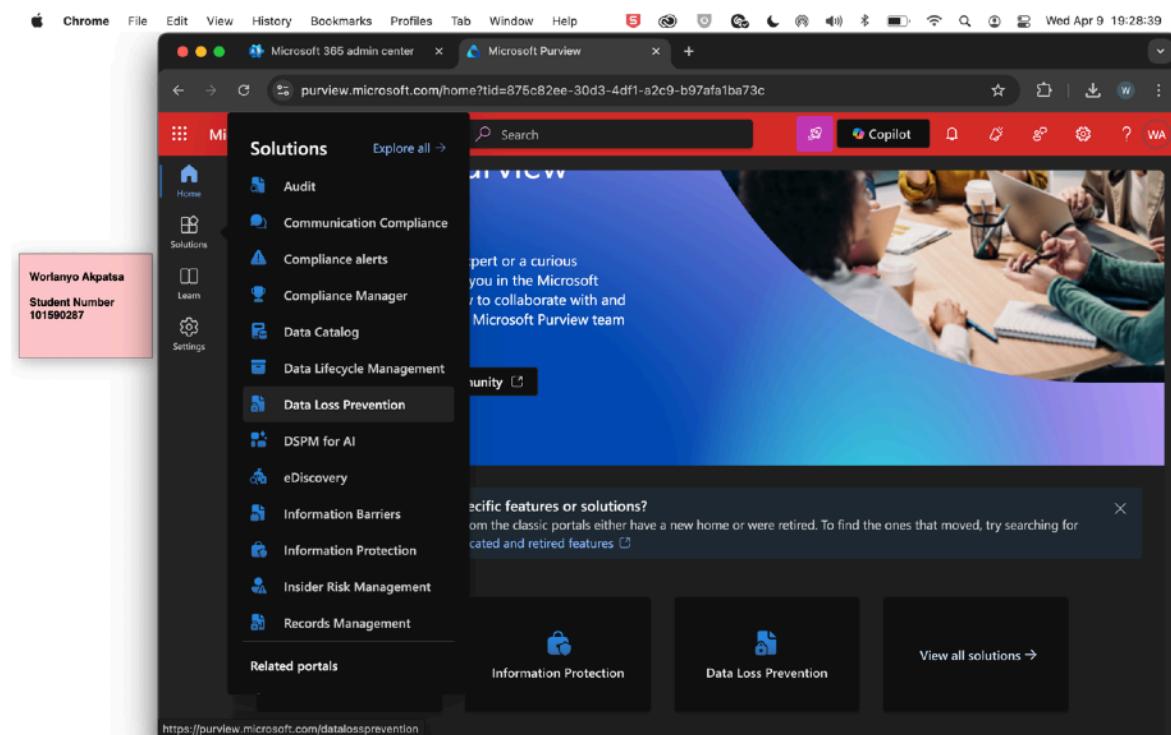
---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 1.2: Create a new DLP policy to protect sensitive information

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



## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Click on “Policies” Subheader

This screenshot shows the Microsoft Purview Data Loss Prevention (DLP) Overview page. The left sidebar has a red box highlighting the 'Data Loss Prevention' section, which contains a 'Policies' link under 'Solutions'. The main content area features a 'Stay informed about DLP' section with links to follow setup guides, read official docs, get news, and watch videos. A callout box at the top right encourages turning on advanced classification.

This screenshot shows the Microsoft Purview Policies page. The left sidebar has a red box highlighting the 'Policies' link under 'Solutions'. The main content area displays a list of policies. At the top, there's a note about setting up billing for Fabric. Below the note, a 'Get started' button is visible, followed by a table showing one item: 'Default Office 365 DLP policy'. The table columns are 'Name', 'Priority', and 'Last modified'.

| Name                          | Priority | Last modified        |
|-------------------------------|----------|----------------------|
| Default Office 365 DLP policy | 0        | Mar 24, 2025 3:48 AM |

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

C: Click on the “+” to Create Policy

The screenshot shows a web browser window for the Microsoft 365 admin center. The URL is [purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The left sidebar has a red box highlighting the user information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area is titled "Policies". It contains two informational cards: one about role group permissions and another about setting up billing for Fabric. Below these cards is a "Create policy" section with a "Create policy" button and a table showing one item: "Default Office 365 DLP policy".

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Policy Creation (Selecting Template = Financial)

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. [Learn more about DLP policy templates](#)

| Regulations              | Canada Financial Data                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Australia Financial Data | Helps detect the presence of information commonly found in financial data, including bank account and credit card numbers. |
| <b>Financial</b>         | <b>Canada Financial Data</b>                                                                                               |
| Medical and health       |                                                                                                                            |
| Privacy                  | France Financial Data                                                                                                      |
| Custom                   | Germany Financial Data                                                                                                     |
|                          | Israel Financial Data                                                                                                      |
|                          | Japan Financial Data                                                                                                       |
|                          | PCI Data Security Standard (PCI DSS)                                                                                       |

Next Cancel

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

#### A: Policy Creation (Naming and Describing Policy)

Worlanyo Akpatsa  
Student Number  
101590287

Template or custom policy

Name

Admin units

Locations

Policy settings

Policy mode

Finish

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name \*

Credit Card DLP

Description

Helps detect the presence of information commonly considered to be financial data in Canada, including bank account numbers and credit cards.

Back Next Cancel

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

| Location                 | Scope              | Actions |
|--------------------------|--------------------|---------|
| Exchange email           | All groups         | Edit    |
| SharePoint sites         | All sites          | Edit    |
| OneDrive accounts        | All users & groups | Edit    |
| Devices                  | All users & groups | Edit    |
| Instances                | All instances      | Edit    |
| On-premises repositories | All repositories   | Edit    |

Choose where to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a web browser window for the Microsoft 365 admin center, specifically the Purview Policies section. The URL is `purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c`. The page title is "Policies | Microsoft Purview". The main content area is titled "Define policy settings" with the sub-instruction: "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." There are two radio button options: "Review and customize default settings from the template." (which lists "Credit Card Number" and "Canada Bank Account Number") and "Create or customize advanced DLP rules." The second option is selected. On the left, there is a sidebar with a navigation tree: "Template or custom policy" (selected), "Name", "Admin units", "Locations", "Policy settings" (selected), "Policy mode", and "Finish". The user's name "Worlanyo Akpatsa" and student number "101590287" are displayed at the top of the sidebar.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Creating custom DLP rules (click create rule)

The screenshot shows a web browser window for the Microsoft 365 admin center, specifically the Policies section under Purview. The URL is purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c. The page title is "Create policy". On the left, there's a sidebar with a red header containing the student's name and ID: "Worlanyo Akpatsa" and "Student Number 101590287". Below this, a vertical list of steps is shown: "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 content area is titled "Customize advanced DLP rules" and contains a sub-section "Create rule" with a "Create rule" button. Below this, a table lists two items:

| Name                                            | Status |
|-------------------------------------------------|--------|
| Low volume of content detected Credit Card DLP  | On     |
| High volume of content detected Credit Card DLP | On     |

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### D: Creating Custom DLP rule (naming rule)

The screenshot shows a web browser window for the Microsoft 365 admin center, specifically the Purview Policies section. The URL in the address bar is `purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afaf1ba73c`. The main content area is titled "Create rule". A sidebar on the left displays the user's name, "Worlanyo Akpatsa", and student number, "101590287". The main form fields include:

- Name \***: Block Credit Card Info in Email
- Description**: A rule to block credit Card information in emails

Below these fields are two expandable sections:

- Conditions**: We'll apply this policy to content that matches these conditions. There is a "+ Add condition" button.
- Exceptions**: We won't apply this rule to content that matches any of these exceptions. There is a "+ Add exception" button.

At the bottom of the form are "Save" and "Cancel" buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the 'Create rule' page in the Microsoft Purview section of the Microsoft 365 admin center. The URL in the browser is `purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c`. The page has a red header bar with the Microsoft Purview logo and a search bar. Below the header, the main content area is titled 'Create rule'. It contains two sections: 'Conditions' and 'Exceptions'. The 'Conditions' section is expanded, showing a 'Content contains' rule with a 'Group name' field set to 'Default' and a 'Group operator' field set to 'Any of these'. There is also a 'Sensitive info types' section with a '+' button. The 'Exceptions' section is collapsed. At the bottom of the page are 'Save' and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Purview Policies interface. On the left, there's a sidebar with the user's name and student number. The main area is titled 'Create rule' under 'Sensitive info types'. It shows a search bar for 'credit card' with one result selected: 'Credit Card Number' by Microsoft Corporation. There are sections for 'Conditions' (Content contains: Group name - Default) and 'Exceptions'.

This screenshot shows the same 'Create rule' interface after changes. The 'Sensitive info types' section now includes 'Credit Card Number' with a dropdown set to 'High confidence' and 'Instance count' set to '1'. The 'Conditions' section remains the same with 'Default' group and 'Any of these' operator.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a web browser window with the Microsoft 365 admin center and Policies | Microsoft Purview tabs open. The main content is the 'Create rule' dialog. On the left, there's a sidebar with the user's name and student number. The main area has a red header bar with the Microsoft Purview logo and a search bar. Below that, the 'Create rule' section is visible. Under 'User notifications', a toggle switch is set to 'On'. A note says 'Use notifications to inform your users and help educate them on the proper use of sensitive info.' Below this, a note states 'Support and behavior for policy tips varies across apps and platforms. [Learn where policy tips are supported](#)'. Under 'Endpoint devices', there are two options: 'Show users a policy tip notification when an activity is restricted' (checked) and 'Customize the notification' (unchecked). Under 'Microsoft 365 files and Microsoft Fabric items', there's a checked checkbox for 'Notify users in Office 365 service with a policy tip or email notifications'. Under 'Email notifications', there's a note 'Preview and edit notification email' and a radio button for 'Notify the user who sent, shared, or last modified the content.' At the bottom are 'Save' and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the 'Create rule' dialog in the Microsoft Purview admin center. On the left, a sidebar displays the user's name (Worlanyo Akpatsa) and student number (101590287). The main area is titled 'Create rule' under 'Endpoint devices'. It includes sections for 'Title' (Email Contains Sensitive Info), 'Content' (This email contains sensitive Financial information), and 'Hyperlink' (Enter hyperlink to use for policy tip's 'Get support' option). Below these, there are sections for 'Microsoft 365 files and Microsoft Fabric items' (Notify users in Office 365 service with a policy tip or email notifications) and 'Email notifications' (Preview and edit notification email). At the bottom are 'Save' and 'Cancel' buttons.

This screenshot shows the same 'Create rule' dialog, but with different configuration settings. Under 'Email notifications', the 'Notify the user who sent, shared, or last modified the content.' option is selected. In the 'Policy tips' section, the 'Customize the policy tip text' checkbox is checked, and the text 'This email contains sensitive Financial information.' is entered into the text area. Other policy tip options like 'Show the policy tip as a dialog for the end user before send' and 'Upload a JSON file containing custom content' are also visible. The bottom of the dialog shows 'User overrides' and 'Save' and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

G: Advanced DLP rule created

The screenshot shows a browser window for the Microsoft 365 admin center, specifically the Policies section under Purview. The URL is [purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The page title is "Policies | Microsoft Purview". On the left, there's a sidebar with the user information "Worlanyo Akpatsa" and "Student Number 101590287". Below this is a navigation tree with the following items:

- Template or custom policy (selected)
- Name
- Admin units
- Locations
- Policy settings** (selected)
- Advanced DLP rules
- Policy mode
- Finish

The main content area is titled "Customize advanced DLP rules". It contains a sub-header: "The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones." Below this is a button "+ Create rule" and a list of existing rules with 3 items.

| Name                                            | Status |
|-------------------------------------------------|--------|
| Low volume of content detected Credit Card DLP  | On     |
| High volume of content detected Credit Card DLP | On     |
| Block Credit Card Info in Email                 | On     |

Under each rule, there are sections for "Conditions" and "Actions".

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### H: Turning Policy on immediately

The screenshot shows a web browser window for the Microsoft 365 admin center, specifically the Microsoft Purview Data Loss Prevention section. The URL in the address bar is `purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c`. The page title is "Policies | Microsoft Purview". On the left, there's a sidebar with the user's name, "Worlanyo Akpatsa", and student number, "101590287". The main content area shows a "Create policy" wizard with the following steps listed on the left:

- Template or custom policy (selected)
- Name
- Admin units
- Locations
- Policy settings
- Policy mode (selected)
- Finish

The right side of the screen 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.

At this time, simulation mode isn't supported for these locations you selected: On-premises file repositories, Microsoft Defender for Cloud Apps

Run the policy in simulation mode  
We'll show you items that match the policy's conditions to help you evaluate its impact. Your data won't be affected; the policy stays off while in simulation mode. [Learn more about simulation mode](#)  
 Show policy tips while in simulation mode.  
 Turn the policy on if it's not edited within fifteen days of simulation

Turn the policy on immediately  
After the policy is created, it'll take up to an hour before any changes are enforced.

Leave the policy turned off  
Decide to test or activate the policy later.

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### I: Review and finish

The screenshot shows a browser window for the Microsoft 365 admin center, specifically the Policies section under Purview. The URL is purview.microsoft.com/datalossprevention/policies?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c. The page title is "Policies | Microsoft Purview". On the left, there's a sidebar with the user's name (Worlanyo Akpatsa) and student number (101590287). The main content area is titled "Review and finish" and contains a summary of the policy settings. A vertical checklist on the left indicates the steps completed: "Template or custom policy" (checked), "Name" (checked), "Admin units" (checked), "Locations" (checked), "Policy settings" (checked), "Policy mode" (checked), and "Finish" (unchecked). The policy details listed are: "The information to protect" (Canada Financial Data, with an "Edit" link), "Name" (Credit Card DLP, with an "Edit" link), "Description" (Helps detect the presence of information commonly considered to be financial data in Canada, including bank account numbers and credit cards, with an "Edit" link), and "Locations" (Exchange email, SharePoint sites, OneDrive accounts, Devices, Microsoft Defender for Cloud Apps). At the bottom are "Back", "Submit" (highlighted in blue), and "Cancel" buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

J: Policy created

The screenshot shows a Microsoft Purview Policies creation page. On the left, there's a sidebar with the user's name and student number. The main area has a green checkmark icon and the text "New policy created". It says "Data loss prevention policy has been created." Below that, under "Next steps", it says "Monitor alerts to review policy matches. Learn about reviewing alerts". Under "Related tasks", there are two items: "Investigate and take action on insider risks and threats" (with a "Start a free 90-day trial to use insider risk management" link) and "Automatically retain or delete sensitive content" (with a "Start a free 90-day trial to use records management" link). A "Done" button is at the bottom.

The screenshot shows the Microsoft Purview Policies overview page. The sidebar includes sections for Solutions (Home, Team, Settings), Data Loss Prevention (Overview, Policies, Alerts, Classifiers, Explorers, Diagnostics), Related solutions (Information Protection, Insider Risk Management), and Copilot. The main area displays a "Policies" section with a brief description and two notifications: one about role group permissions and another about pay-as-you-go billing. Below this is a table listing two policies: "Default Office 365 DLP policy" and "Credit Card DLP".

| Name                          | Priority | Last modified        | Owner      |
|-------------------------------|----------|----------------------|------------|
| Default Office 365 DLP policy | 0        | Mar 24, 2025 3:48 AM | Office 365 |
| Credit Card DLP               | 1        | Apr 9, 2025 7:59 PM  | Office 365 |

## Microsoft 365 Identity and Services – Enterprise Administration

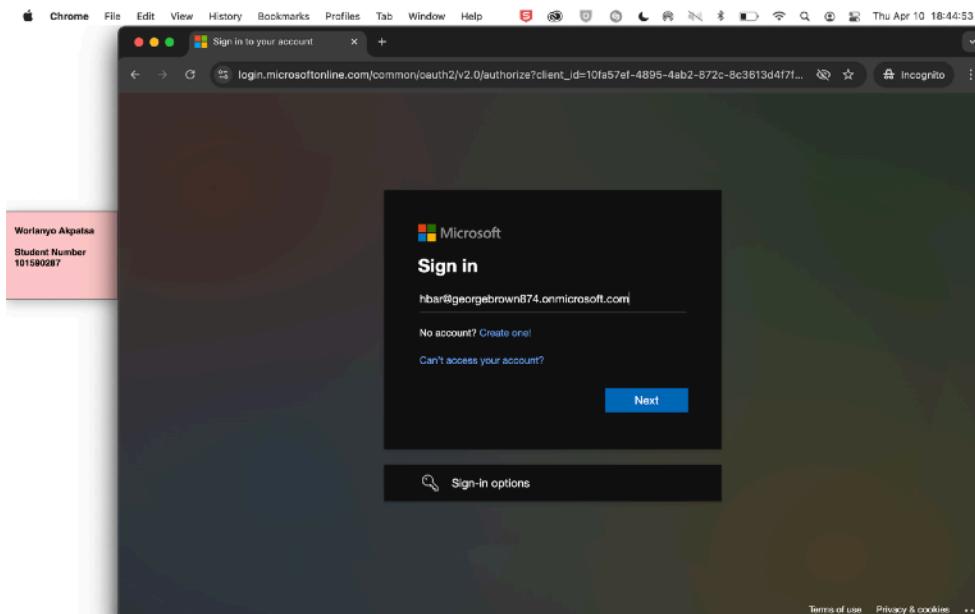
---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

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



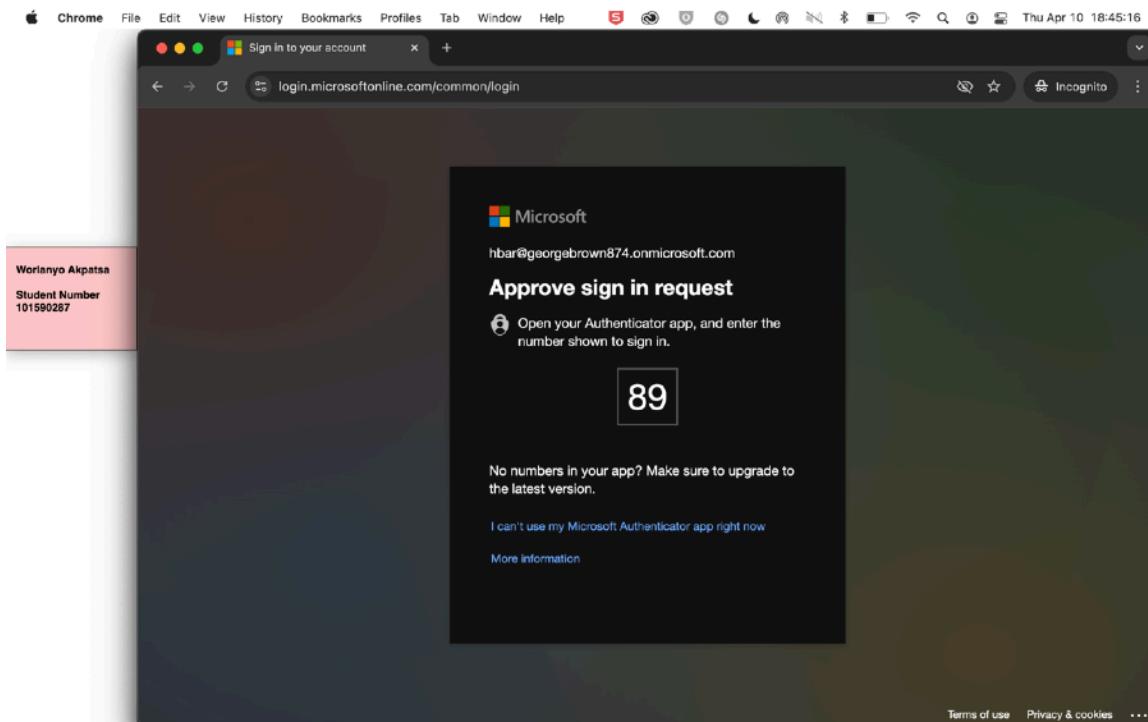
## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: MultiFactor Authentication



## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

C: User's Outlook homepage

The screenshot shows the Microsoft 365 admin center Outlook homepage. On the left, there is a sidebar with a red header bar containing the user's name and student number. The main area has a red header bar with the word "Outlook". Below the header, there is a toolbar with various icons. The left pane shows a navigation menu with sections like "Favorites" and "Folders". The main pane displays the "Inbox" with several messages listed. One message from "Microsoft 365 Message center" is highlighted, showing a preview of the weekly digest. To the right of the inbox, there is a "Message center announcements" section with a summary of recent changes.

WORLANYO

New mail

Inbox

Sent Items

Drafts

Favorites

Inbox

Sent Items

Drafts

Deleted Items

Junk Email

Notes

Archive

Conversation Hist...

Search Folders

Inbox

Yesterday

Microsoft 365

Welcome to your ...

This week

Microsoft 365 Message center

Weekly digest: Mi...

Last week

Microsoft 365

Welcome to your Micr...

WorlaPlan

You've joined the Worl...

Worlanyo Akpatsa

EMAIL TO SHARED MA...

Weekly digest: Microsoft service updates

Microsoft 365 Message center <o365mc@microsoft.co...

To: Hamish Bar

Mon 4/7/2025 2:17 AM

Some content in this message has been blocked because the sender isn't in your Safe senders list.

Trust sender Show blocked content

As a new admin to the Microsoft 365 admin center, you'll get weekly emails from the message center about upcoming changes to your services until April 30, 2025. Update your preferences to continue getting emails like this one. Go to preferences

Message center announcements

March 31, 2025 - April 6, 2025

GEORGEBROWN

Major updates

DNS Provisioning Change

MC198624 | April 4 - We're making some changes to DNS provisioning of A records for all new Accepted Domains provisioned after July 1st, 2025. Between July 1st and August 1st, 2025, we will gradually switch provisioning of all A records for new Accepted Domains into the new subdomains under ms.outlook.com. We are doing this to reduce the friction of adding

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Sending email with sensitive info

The screenshot shows the Microsoft 365 admin center Mail interface in a web browser. The left sidebar displays the user profile (Worlanyo Akpatsa, Student Number 101590287) and navigation links for Favorites, Folders, and other mailbox items. The main pane shows the inbox with several messages from Microsoft 365 and Worlanyo Akpatsa. On the right, a compose window is open, addressed to 'Bruno Mercer-Bermac'. The message body contains a draft of an email:

Hi Bruno,  
Go buy yourself a new computer, I have a Scotiabank account.  
Here's the card number: 4111 1111 1111 1111.  
Yours sincerely,  
Hamish.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A screenshot of a Microsoft 365 admin center window titled "WORLANYO". The left sidebar shows navigation options like Home, View, Help, Message, Insert, Format text, Draw, and Options. Under "Folders", the "Inbox" folder is selected, showing 1 item. The inbox list includes several messages from Microsoft 365 and one from "Worlanyo Akpatsa". A draft message is open on the right, addressed to "Bruno Mercer-Bermac". The message body contains a credit card number: "Go buy yourself a new computer. I have a Scotiabank account. Here's the card number: 4111 1111 1111 1111". The message is saved as a draft at 6:53 PM.

A screenshot of a Microsoft 365 admin center window titled "WORLANYO". The left sidebar shows navigation options like Home, View, Help, Message, Insert, Format text, Draw, and Options. Under "Folders", the "Inbox" folder is selected, showing 1 item. The inbox list includes several messages from Microsoft 365 and one from "Worlanyo Akpatsa". A draft message is open on the right, addressed to "Mercer-Bermac". A policy tip message is displayed: "Policy tip: Your email message conflicts with a policy in your organization. Learn more". Below it, a warning message states: "This message appears to contain the following sensitive information: Credit Card Number". A "Report" button is available. The message body contains a credit card number: "Go buy yourself a new computer. I have a Scotiabank account. Here's the card number: 4111 1111 1111 1111". The message is saved as a draft at 6:53 PM.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a Microsoft 365 admin center interface with a red header bar. The left sidebar displays navigation links such as Home, View, Help, New mail, Favorites (Inbox, Sent Items, Drafts), Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Notes, Archive, Conversation History, Search Folders), and other icons for Groups, Devices, and Reports. The main content area shows the 'Inbox' tab selected. A message from 'Microsoft Outlook' titled 'Notification: MY CREDIT CARD INFO' is highlighted. The message body states: 'Your email message conflicts with a policy in your organization. Issues: • Message contains the following sensitive information: Credit Card Number'. Below the message are 'Reply' and 'Forward' buttons.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### ***Task 1 Summary***

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

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

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

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

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

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

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

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

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

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

---

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

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

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

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

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

## Microsoft 365 Identity and Services – Enterprise Administration

---

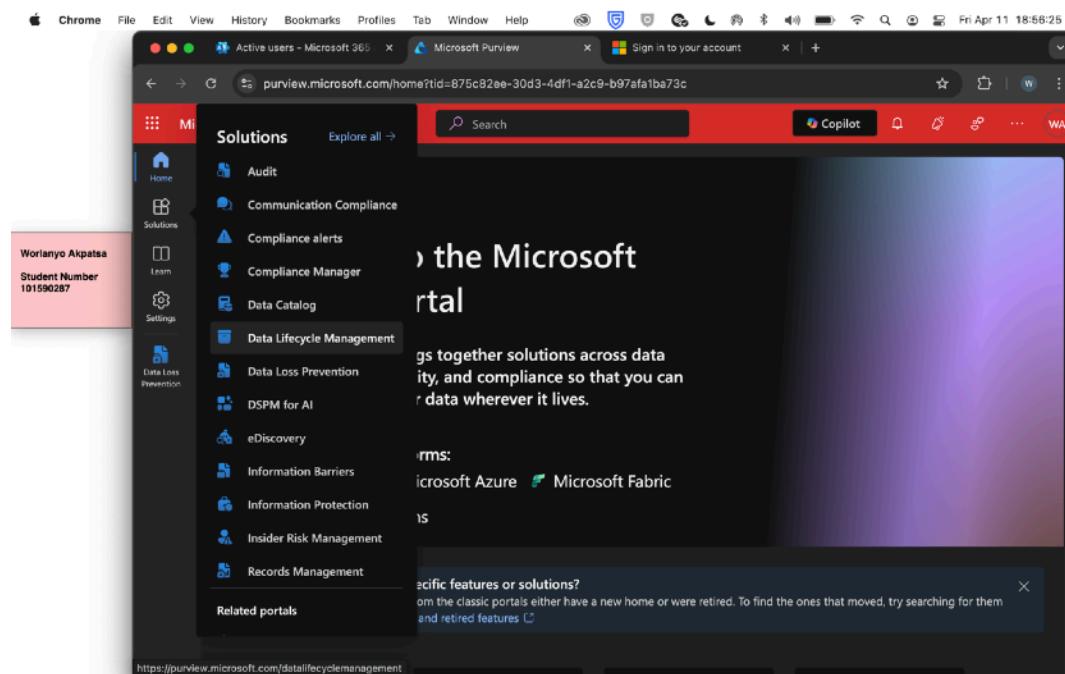
Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### TASK 2: IMPLEMENT RETENTION POLICIES

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

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



## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: Data Lifecycle Management Overview Page

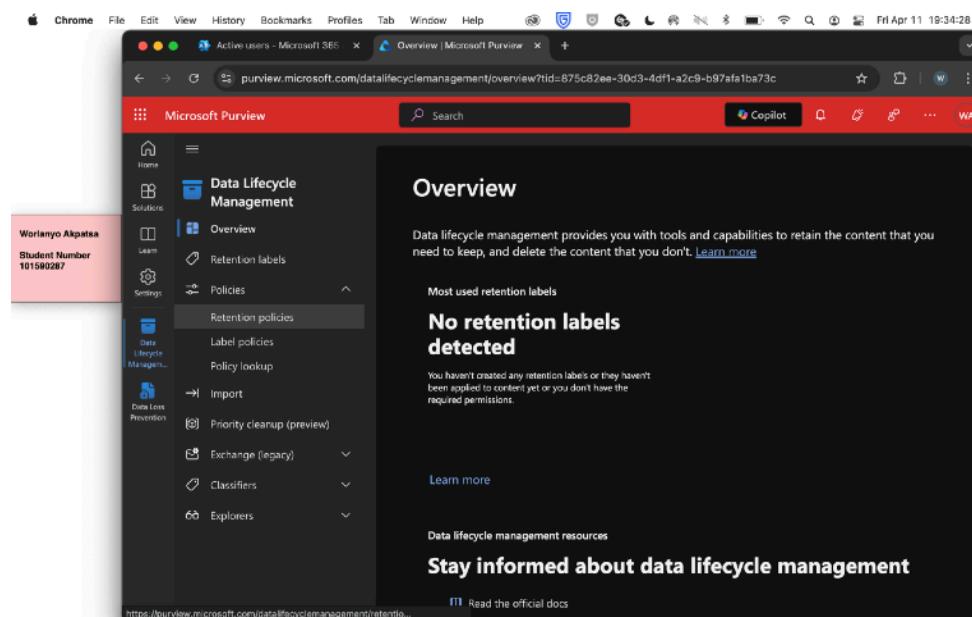
The screenshot shows a Microsoft Chrome browser window with the URL [purview.microsoft.com/datalifecyclemanagement/overview?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://purview.microsoft.com/datalifecyclemanagement/overview?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The page title is "Overview | Microsoft Purview". The left sidebar has a red header bar with the user's name "Worlanyo Akpatsa" and student number "101590287". The sidebar includes sections for Home, Solutions, Learn, Settings, Data Lifecycle Management (selected), Data Loss Prevention, and Explorers. The main content area has a dark background. It features a large heading "Overview" and a sub-section "No retention labels detected" with the message "You haven't created any retention labels or they haven't been applied to content yet or you don't have the required permissions." There is also a "Learn more" link and a "Data lifecycle management resources" section with a "Read the official docs" link.

## Microsoft 365 Identity and Services – Enterprise Administration

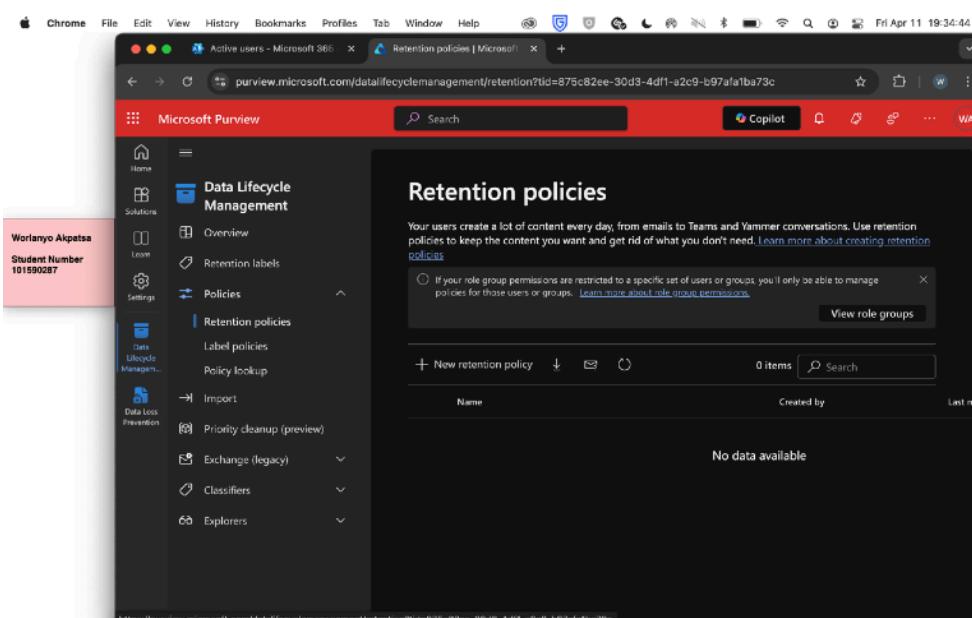
Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

C: Click the policies subheader and select Retention Policies



The screenshot shows a Microsoft Purview interface in a web browser. The left sidebar has a red highlight on the user information: "Worlanyo Akpatsa" and "Student Number 101590287". Under "Data Lifecycle Management", the "Policies" section is expanded, and "Retention policies" is selected. The main content area is titled "Overview" and discusses data lifecycle management tools for retaining content. It states "No retention labels detected" and provides a link to "Read the official docs".



The screenshot shows the "Retention policies" page from Microsoft Purview. The left sidebar is identical to the previous screenshot. The main content area is titled "Retention policies" and explains how users can manage content using retention policies. A message indicates that role group permissions are restricted, and a "View role groups" button is shown. Below this, there's a search bar and a table with columns for "Name", "Created by", and "Last modified". The table displays the message "No data available".

## Microsoft 365 Identity and Services – Enterprise Administration

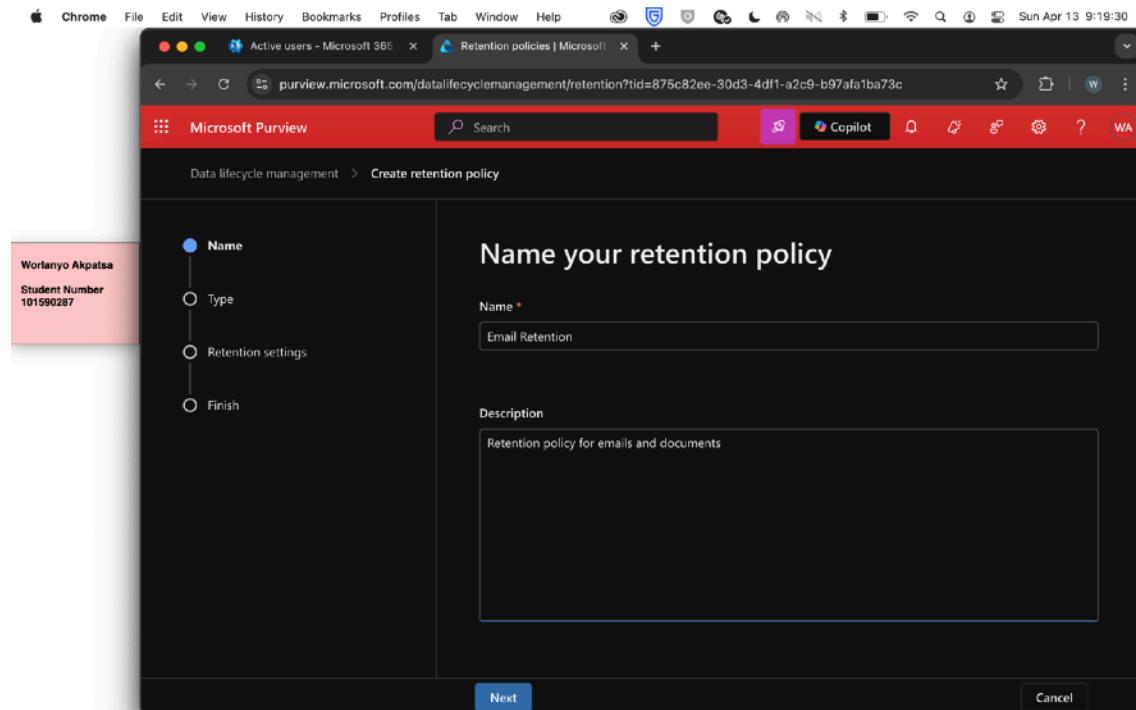
---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 2.2: Create a new retention policy for emails and documents

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



## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Choosing type of retention policy (static)

The screenshot shows a web browser window for Microsoft Purview Data Lifecycle Management. The URL is [purview.microsoft.com/datalifecyclemanagement/retention?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://purview.microsoft.com/datalifecyclemanagement/retention?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The page title is "Retention policies | Microsoft". The left sidebar shows the user's name (Worlanyo Akpatsa) and student number (101590287). The main content area is titled "Choose the type of retention policy to create". It explains that adaptive scopes can be specified dynamically or selected individually. Two options are shown: "Adaptive (available with Microsoft 365 E5 license or equivalent)" and "Static". The "Static" option is selected. At the bottom are "Back", "Next", and "Cancel" buttons.

# Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

## 2.3: Apply the policy to a specific group of users

C: Choosing locations for where retention policy would apply

This screenshot shows the Microsoft Purview Data Lifecycle Management interface. On the left, a sidebar for 'Worlanyo Akpatsa' displays 'Student Number 101590287'. The main panel is titled 'Edit retention policy' under 'Data lifecycle management'. A navigation tree on the left includes 'Name', 'Type' (selected), 'Locations', 'Retention settings', and 'Finish'. The right side is titled 'Exchange mailboxes' and shows a list of selected mailboxes. The 'Status' column has checkboxes for 'On' or 'Off' next to each location type: 'Exchange mailboxes', 'Share classic communication sites', 'OneDrive accounts', and 'Microsoft 365 Group mailboxes'. The 'Location' column lists the mailbox names and their respective email addresses. Buttons at the bottom include 'Back', 'Next', 'Done', and 'Cancel'.

This screenshot continues the 'Edit retention policy' process. The sidebar remains the same. The main panel now shows the 'Applicable Content' section. It includes a note about setting up data connectors to import content from non-Microsoft apps like Slack and WhatsApp. The 'Included' column lists four categories: '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.' (2 mailboxes), '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)' (All sites), 'All files in users' OneDrive accounts.' (All user accounts), and '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 sites.' (All Microsoft 365 groups). Buttons at the bottom include 'Back', 'Next', and 'Cancel'.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a Microsoft Purview Data Lifecycle Management interface for editing a retention policy. On the left, a sidebar lists steps: Name (done), Type (done), Retention settings (selected), and Finish (not yet done). The main area is titled "Decide if you want to retain content, delete it, or both". It contains a radio button for "Retain items for a specific period" (selected) with a dropdown set to "5 years". Below this, under "Start the retention period based on", there's a dropdown set to "When items were created". Under "At the end of the retention period", the "Delete items automatically" option is selected. There are also options for "Do nothing" and "Retain items forever". At the bottom, there are "Back", "Next", and "Cancel" buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

E: Review and finish

The screenshot shows a Microsoft Purview interface for editing a retention policy. On the left, a sidebar displays the user's name (Worlanyo Akpatsa) and student number (101590287). A vertical progress bar on the right indicates the steps completed: Name (checkmark), Type (checkmark), Retention settings (checkmark), and Finish (checkmark). The main content area is titled 'Review and finish' and contains the following details:

- Policy name:** Email Retention ([Edit](#))
- Description:** Retention policy for emails and documents ([Edit](#))
- Locations to apply the policy:**
  - Exchange mailboxes (2 Recipients)
  - SharePoint classic and communication sites (All Sites)
  - OneDrive accounts (All Sites)
  - Microsoft 365 Group mailboxes & sites (All Groups)[Edit](#)
- Retention settings:**
  - Retain items for 5 years based on when they were created
  - Delete items at end of retention period[Edit](#)

At the bottom, there are 'Back', 'Submit', and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

F: Retention Policy created

The screenshot shows a browser window for Microsoft Purview Data Lifecycle Management. The URL is [purview.microsoft.com/datalifecyclemanagement/retention?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://purview.microsoft.com/datalifecyclemanagement/retention?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The page title is "Retention policies | Microsoft". On the left, there's a sidebar with the user's name, Worlanyo Akpatsa, and student number, 101590287. A vertical checklist on the right indicates the steps completed: Name (green checkmark), Type (green checkmark), Retention settings (green checkmark), and Finish (green checkmark). The main content area displays a success message: "You successfully created a retention policy". It also includes a note: "Allow up to a week for the retention policy to be enforced." Below this are sections for "Related tasks" (Create another retention policy, Get started button), "Try adaptive retention policies for free for 90 days" (Learn more button), and "Create a retention label" (Get started button). At the bottom is a "Done" button.

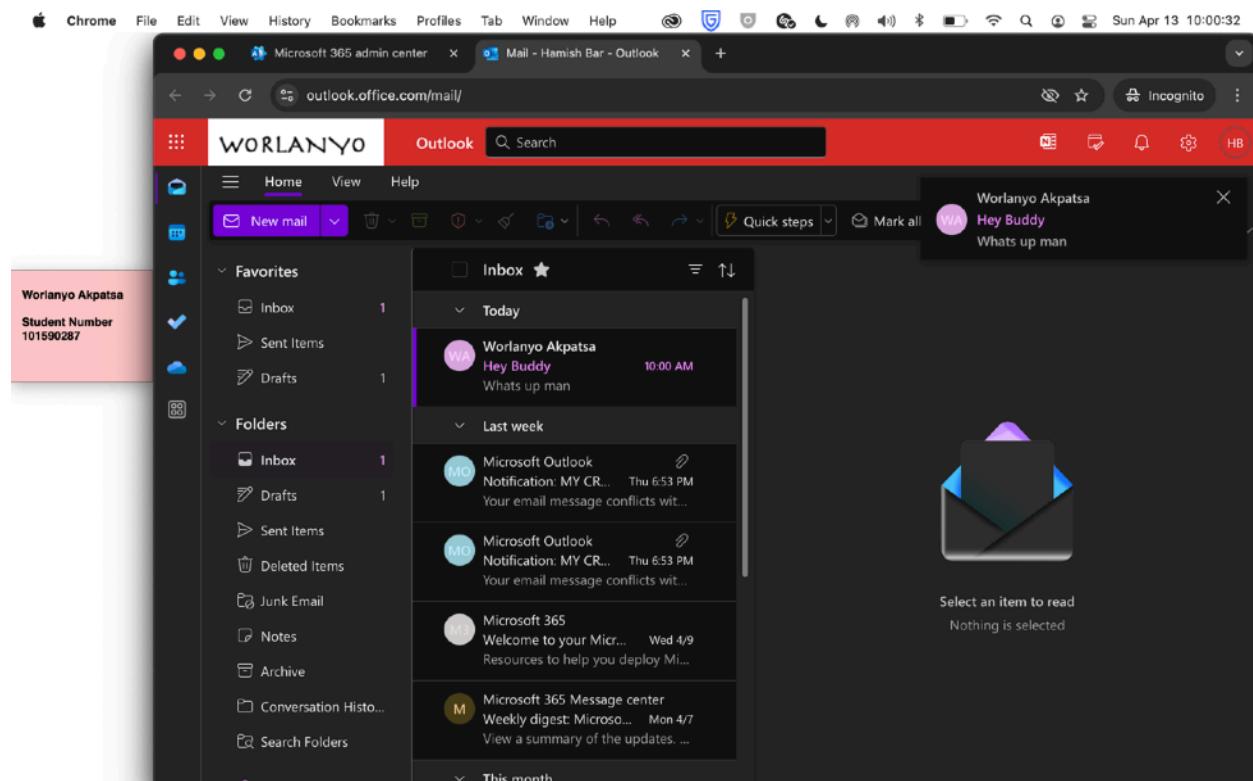
## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

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



## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a Microsoft 365 admin center interface with a Mail - Hamish Bar - Outlook tab. The left sidebar displays navigation links such as Home, View, Help, New mail, Favorites (Inbox, Sent Items, Drafts), Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Notes, Archive, Conversation History, Search Folders), and other options like Go to Microsoft 365 admin center and Log off.

The main area shows the inbox under the "Inbox" heading. It lists several messages:

- Hey Buddy (Today) - From Worlanyo Akpatsa at 10:00 AM. The message content is "Whats up man". A retention label "Retention: 5 Year Delete (5 years) Expires: Fri 4/12/2030 6:00 AM" is visible above the message preview.
- Microsoft Outlook (Last week) - Notification: MY CR... Thu 6:53 PM. Message content: "Your email message conflicts with another message you sent or received."
- Microsoft Outlook (Last week) - Notification: MY CR... Thu 6:53 PM. Message content: "Your email message conflicts with another message you sent or received."
- Microsoft 365 (This month) - Welcome to your Micr... Wed 4/9. Message content: "Resources to help you deploy Mi...".
- Microsoft 365 Message center (This month) - Weekly digest: Microso... Mon 4/7. Message content: "View a summary of the updates. ...".

At the bottom right of the inbox view, there are "Reply" and "Forward" buttons.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### ***Task 2 Summary***

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

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

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

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

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

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

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### TASK 3: CONFIGURE AND MONITOR SECURITY ALERTS

#### 3.1: Access the security center (MS Defender)

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

The screenshot shows the Microsoft 365 Admin Center homepage. The left sidebar has a red header bar with the user's name 'WORLANYO' and student number '101590287'. Below this, under 'Admin centers', the 'Security' option is highlighted with a blue icon and the text 'Security'. Other options include 'Compliance', 'Microsoft Intune', 'Identity', 'Exchange', 'SharePoint', 'Power Platform', and 'All admin centers'. At the bottom of the sidebar, there is a link to 'Customize navigation'. The main content area features a greeting 'Good evening, Worlanyo Akpatsa' and a section titled 'For organizations like yours' with a callout for 'Set up email with a custom domain'. Below this is a 'Your organization' section with tabs for 'Users', 'Products', 'Upcoming changes (5)', 'Learn', 'Setup', 'Help & support', and 'Give Feedback'. There are also buttons for '+ Add user', 'Reset password', and 'Assign phone numbers'. A search bar at the bottom right says 'Search your users list'.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Defender Homepage

The screenshot shows a Microsoft Defender homepage in a web browser. The URL in the address bar is [security.microsoft.com/homepage?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c](https://security.microsoft.com/homepage?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c). The page title is "Home - Microsoft Defender". On the left, there is a sidebar with a user profile for "WORLANYO" and "Worlanyo Akpatsa, Student Number 101590287". The sidebar includes navigation links for "Exposure management", "Investigation & response", "Threat intelligence", "Assets", "Microsoft Sentinel", "Endpoints", "Email & collaboration", "Cloud apps", "SOC optimization", and "Reports". The main content area features a large "Welcome to Microsoft Defender" heading. Below it, there are sections for "Intro", "Next steps", and "Give feedback". A call-to-action button says "Next". At the bottom, there are cards for "SOC optimization" (with "Your optimization data" and "0 automation rules") and "Microsoft Sentinel automation". The top of the browser window shows the standard Mac OS X menu bar with "Chrome", "File", "Edit", etc., and the system status bar showing "Sun Apr 13 19:40:11".

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

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

The screenshot shows the Microsoft Defender interface in a web browser. The left sidebar has a red highlight on the 'Email & collaboration' section, which is currently selected. Under 'Email & collaboration', the 'Policies & rules' option is also highlighted. The main content area displays the 'Welcome to Microsoft Defender' page. A tooltip for 'Policies & rules' is visible, stating: 'Configure security policies for email and other Microsoft 365 workspaces.' To the right, there's a section for 'Microsoft Sentinel automation' with a count of '0 automation rules'.

## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B Select Alert Policy

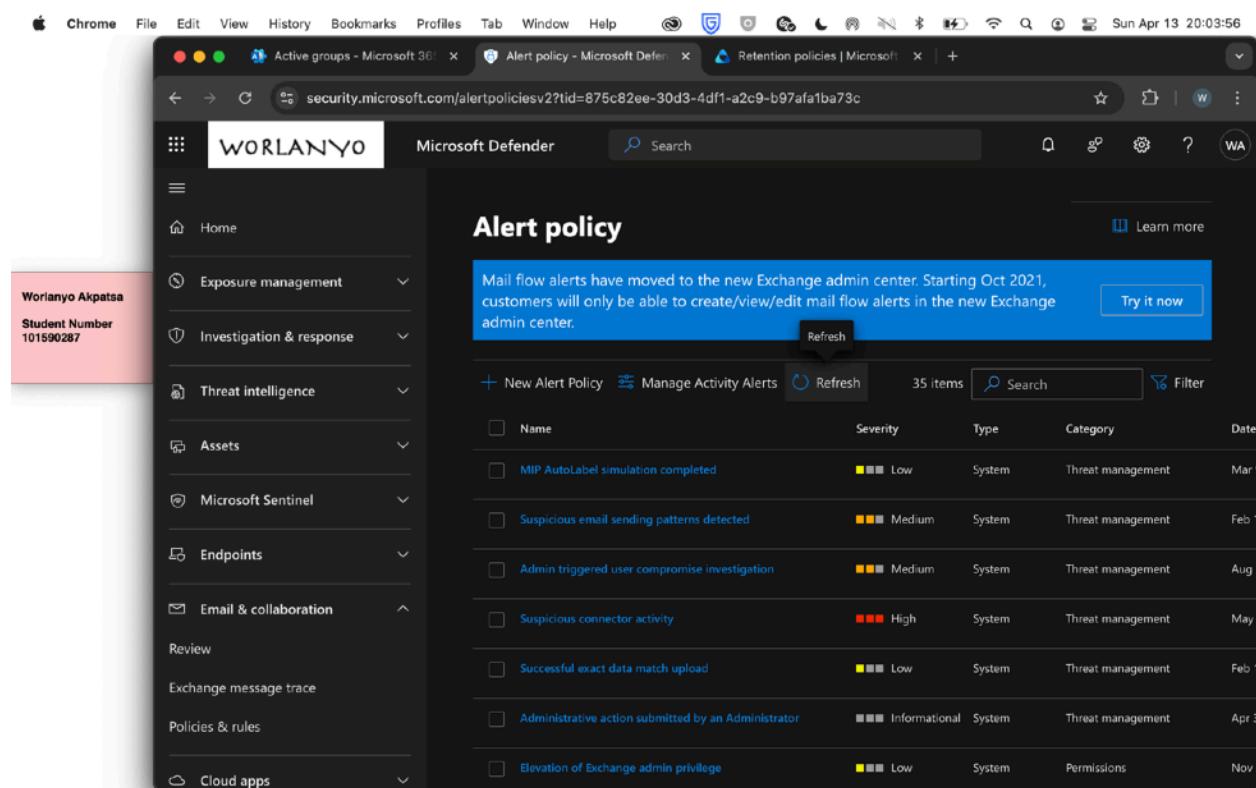
The screenshot shows a Microsoft Defender interface in a web browser. The left sidebar has a red highlight over the user information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area is titled "Policies & rules" and contains the following text: "Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization." Below this, there are four sections: "Name" (dropdown), "Threat policies", "Alert policy" (which is highlighted with a blue bar at the bottom of the list), and "Activity alerts". At the bottom of the page, the URL is visible: <https://security.microsoft.com/securitypoliciesandrules?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c>.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Click New Alert Policy



The screenshot shows the Microsoft Defender interface for managing alert policies. On the left, there's a navigation sidebar with sections like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Endpoints, Email & collaboration, and Cloud apps. A red box highlights the 'Worlanyo Akpatsa' user profile in the sidebar. The main area is titled 'Alert policy' and displays a message about mail flow alerts moving to the Exchange admin center. Below this, a table lists 35 items, each with a checkbox, name, severity (Low, Medium, High), type (System, Threat management, Informational), category, and date. One alert is highlighted: 'MIP AutoLabel simulation completed' (Medium, System, Threat management, Mar 9).

| Name                                                | Severity      | Type   | Category          | Date  |
|-----------------------------------------------------|---------------|--------|-------------------|-------|
| MIP AutoLabel simulation completed                  | Medium        | System | Threat management | Mar 9 |
| Suspicious email sending patterns detected          | Medium        | System | Threat management | Feb 1 |
| Admin triggered user compromise investigation       | Medium        | System | Threat management | Aug 3 |
| Suspicious connector activity                       | High          | System | Threat management | May 6 |
| Successful exact data match upload                  | Low           | System | Threat management | Feb 1 |
| Administrative action submitted by an Administrator | Informational | System | Threat management | Apr 3 |
| Elevation of Exchange admin privilege               | Low           | System | Permissions       | Nov 2 |

## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the 'New Alert Policy' configuration interface. On the left, a sidebar lists navigation options: Home, Active groups, Security Center, Threat & Compliance, Microsoft Defender, and Retention policies. A red box highlights the 'WORLANYO' profile section, which displays the student's name and ID. The main panel is titled 'New Alert Policy' and contains the following fields:

- Name your alert:** The 'Name' field is populated with 'Email Forward Alert'.  
Description: 'Alert Policy for email forward alert'.
- Severity:** Set to 'Medium'.
- Category:** Set to 'Mail flow'.

At the bottom right are 'Next' and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a web browser window for Microsoft Defender, specifically the 'Alert policy' section. The URL in the address bar is `security.microsoft.com/alertpoliciesv2?id=875c82ee-30d3-4df1-a2c9-b97afa1ba73c`. The page title is 'New Alert Policy'. On the left, there's a sidebar with icons for Home, Groups, Protection, Threats, and Policies. A red box highlights the 'Worlanyo Akpatsa' and 'Student Number 101590287' information. The main content area has a flowchart:

- Name your alert (checked)
- Create alert settings (selected)
- Set your recipients
- Review your settings

To the right, under 'Choose an activity, conditions and when to trigger the alert', it says: 'You can only choose one activity but you can add conditions to refine what we'll detect.' Below that is a section titled 'What do you want to alert on?' with a dropdown menu set to 'Activity is' and 'Created mail forward/redirect rule'. A note below says 'User created an inbox rule to forward or redirect mails.' There are 'Add condition' and 'Next' buttons at the bottom.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 3.3: Configure alert notifications to be sent to an administrator

A: Sending alert notifications to admin

The screenshot shows a 'New Alert Policy' configuration interface. On the left, a sidebar lists navigation options: Active groups, Alert policy (selected), Retention policies, and others like Active users, Audit logs, and Compliance. A red box highlights the 'Alert policy' tab. The main area has a title 'New Alert Policy' and a progress bar with four steps: 'Name your alert' (completed), 'Create alert settings' (completed), 'Set your recipients' (in progress, indicated by a blue dot), and 'Review your settings' (not yet started). To the right, under 'Decide if you want to notify people when this alert is triggered', there is a checked checkbox for 'Opt-In for email notifications'. Below it, an 'Email recipients' field contains the email address 'WorlanyoAkpatsa@GeorgeBROWN8...'. A dropdown menu for 'Daily notification limit' is set to 'No limit'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Reviewing settings and turning policy on immediately

The screenshot shows a Microsoft Defender interface for creating a new alert policy. On the left, a sidebar displays the user's name (Worlanyo Akpatsa) and student number (101590287). The main area is titled 'New Alert Policy' and contains four steps: 'Name your alert', 'Create alert settings', 'Set your recipients', and 'Review your settings'. The 'Review your settings' step is currently active. The 'Name your alert' section includes fields for 'Name' (Email Forward Alert), 'Description' (Alert Policy for email forward alert), 'Severity' (Medium), and 'Category' (Mail flow). The 'Create alert settings' section has an 'Edit alert creation' link. The 'Set your recipients' section has an 'Edit recipient set' link. At the bottom, a question asks 'Do you want to turn the policy on right away?' with two options: 'No, keep it off. I will turn it on later.' (unchecked) and 'Yes, turn it on right away.' (checked). Buttons for 'Back', 'Submit', and 'Cancel' are at the bottom.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

C: Alert policy created

The screenshot shows a Microsoft Defender interface for managing alert policies. On the left, there's a sidebar with navigation links like Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Endpoints, Email & collaboration, and Cloud apps. A pink sidebar on the far left displays the user's name (Worlanyo Akpatsa) and student number (101590287). The main content area is titled "Alert policy". It features a message about mail flow alerts moving to the new Exchange admin center. Below this is a table listing 36 items. The columns include Name, Severity (with a color-coded scale from green to red), Type, Category, and Date. Some examples of alerts listed are "Email Forward Alert" (Medium, Custom, Mail flow, April 1), "MIP AutoLabel simulation completed" (Low, System, Threat management, March 9), and "Suspicious email sending patterns detected" (Medium, System, Threat management, Feb 1).

| Name                                                | Severity      | Type   | Category          | Date  |
|-----------------------------------------------------|---------------|--------|-------------------|-------|
| Email Forward Alert                                 | Medium        | Custom | Mail flow         | Apr 1 |
| MIP AutoLabel simulation completed                  | Low           | System | Threat management | Mar 9 |
| Suspicious email sending patterns detected          | Medium        | System | Threat management | Feb 1 |
| Admin triggered user compromise investigation       | Medium        | System | Threat management | Aug 2 |
| Suspicious connector activity                       | High          | System | Threat management | May 8 |
| Successful exact data match upload                  | Low           | System | Threat management | Feb 1 |
| Administrative action submitted by an Administrator | Informational | System | Threat management | Apr 3 |

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A: Logging into Outlook as another user

The screenshot shows a Microsoft 365 admin center interface with a red header bar. The left sidebar displays the user profile 'WORLANYO' and a list of folders: Favorites (Inbox, Sent Items, Drafts), Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Notes, Archive, Conversation History, Search Folders). The main area shows the 'Inbox' tab with several messages listed under 'Today'. One message is selected, showing a preview: 'Hey Buddy' from 'Worlanyo Akpatsa' at 10:00 AM, with the body 'Whats up man'. Below the inbox, there are sections for 'Last week', 'This month', and 'Upcoming'.

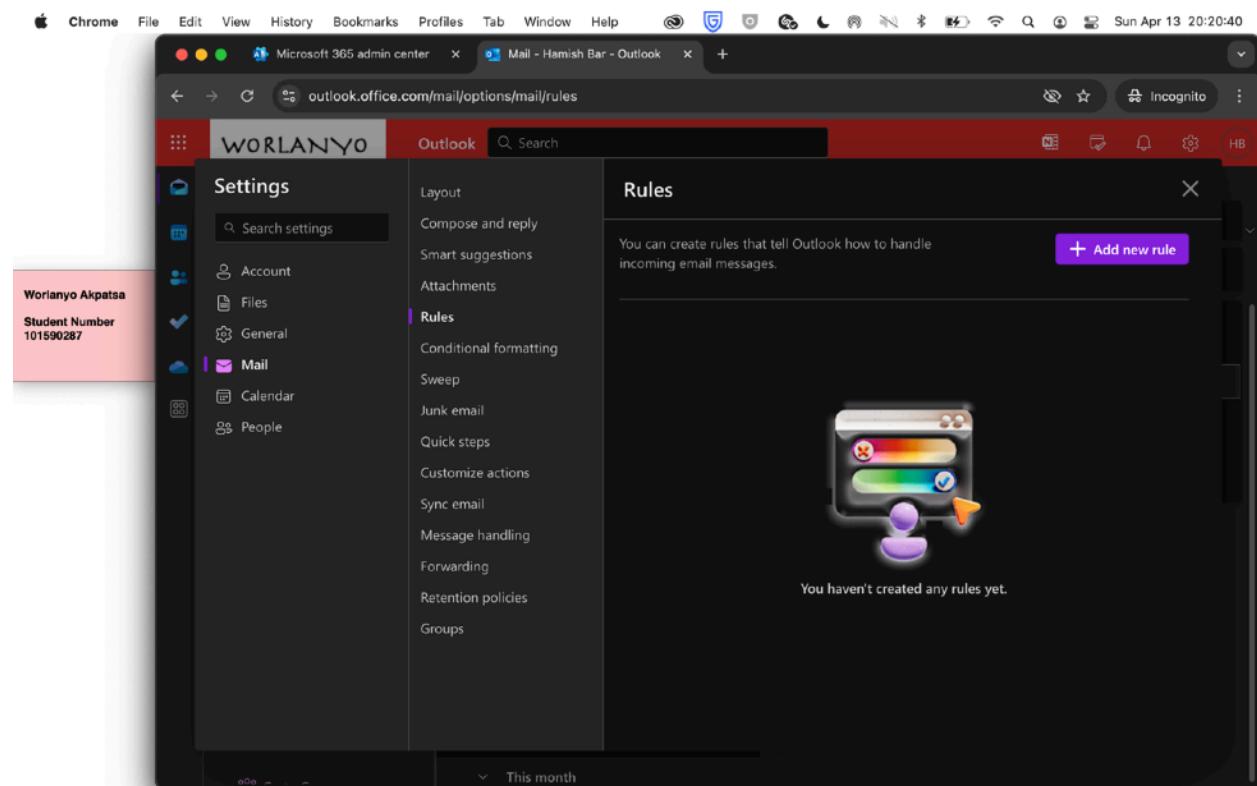
## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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



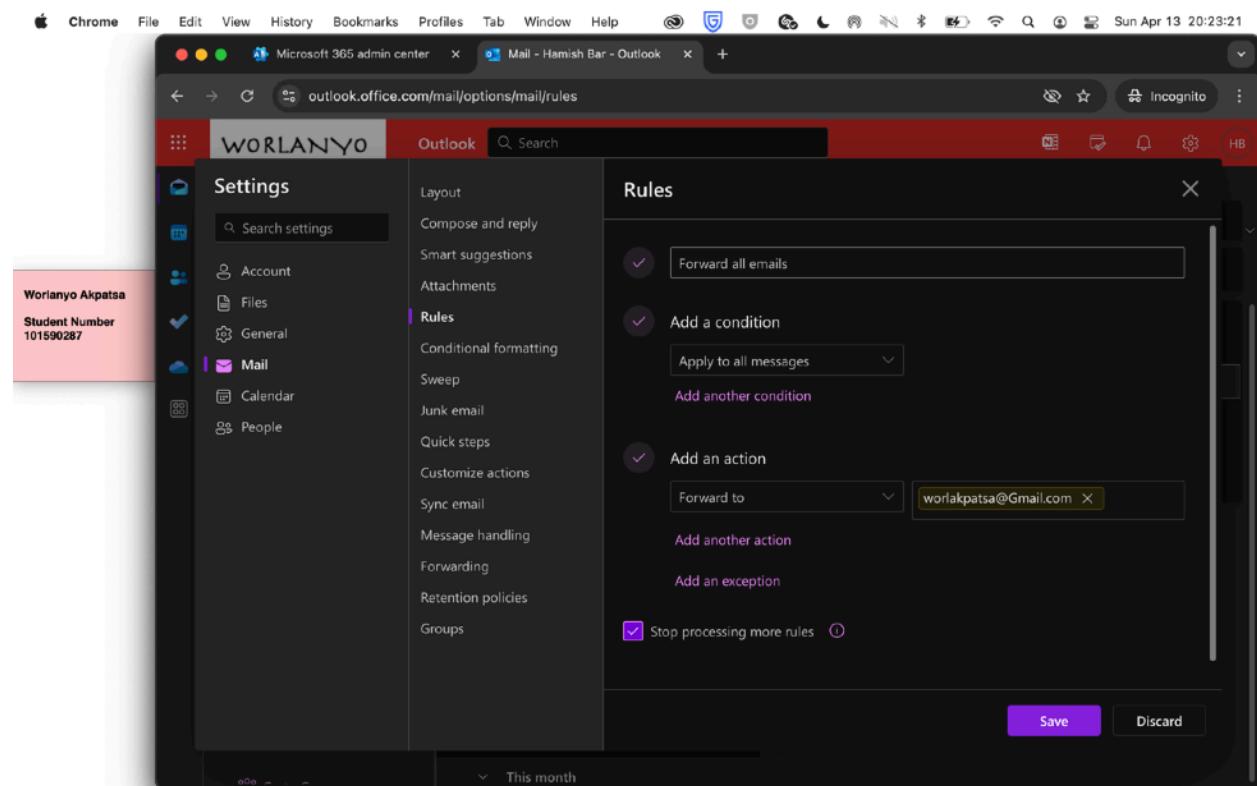
## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

C: Creating rule to forward all emails



## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Go back to Microsoft Defender Portal Homepage for Admin

The screenshot shows a Microsoft Defender portal page in a web browser. The URL in the address bar is <https://security.microsoft.com/homepage?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c>. The page title is "Home - Microsoft Defender". On the left, there is a sidebar with a user profile for "Worlanyo Akpatsa" (Student Number 101590287) and a navigation menu with sections like "Exposure management", "Investigation & response", "Incidents & alerts", "Hunting", "Actions & submissions", "Secure score", "Partner catalog", and "Threat intelligence". The "Threat intelligence" section is expanded, showing "Threat analytics", "Intel management", "Intel profiles", and "Intel explorer". The main content area displays the "Welcome to Microsoft Defender" message, an "Intro" section, and a call-to-action button labeled "Next". The status bar at the bottom shows the URL again.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A screenshot of a web browser displaying the Microsoft Defender console. The URL is security.microsoft.com/alerts?tid=875c82ee-30d3-4df1-a2c9-b97afafba73c. The page has a dark theme with a central illustration of a lit candle. The left sidebar shows navigation categories: Home, Exposure management, Investigation & response, Incidents & alerts, Threat intelligence, and Partner catalog. Under 'Investigation & response', 'Incidents & alerts' is expanded, showing 'Incidents', 'Alerts' (which is selected and highlighted in blue), 'Email & collaboration alerts', 'Hunting', 'Actions & submissions', 'Secure score', and 'Partner catalog'. Under 'Alerts', there are sub-options: 'Incidents', 'Email & collaboration alerts', 'Hunting', 'Actions & submissions', 'Threat intelligence', and 'Intel management'. A message in the center says 'Hang on! We're preparing new spaces for your data and connecting them.' Below it, a note says 'This takes a few minutes. When we're done, your data will gradually consolidate and light up the console in the next few hours. Learn about Microsoft Defender XDR'. The status bar at the bottom indicates the URL https://security.microsoft.com/alerts?tid=875c82ee-30d3-4df1-a2c9-b97afafba73c.

A screenshot of a web browser displaying the Microsoft Defender console. The URL is security.microsoft.com/alerts?tid=875c82ee-30d3-4df1-a2c9-b97afafba73c. The page has a dark theme with a central illustration of a lit candle. The left sidebar shows navigation categories: Home, Exposure management, Investigation & response, Incidents & alerts, Threat intelligence, and Partner catalog. Under 'Investigation & response', 'Incidents & alerts' is expanded, showing 'Incidents', 'Alerts' (which is selected and highlighted in blue), 'Email & collaboration alerts', 'Hunting', 'Actions & submissions', 'Threat intelligence', and 'Learning hub'. Under 'Alerts', there are sub-options: 'Incidents', 'Email & collaboration alerts', 'Hunting', 'Actions & submissions', 'Threat intelligence', and 'Intel management'. The main content area displays a table header for 'Alerts' with columns: 'Incidents', 'Export', '1 Week', '0 Alerts', 'Search for name or ID', and 'Customize columns'. Below the header, there is a 'Filter set' section with a 'Add filter' button. The table body is empty, showing only the column headers. The status bar at the bottom indicates the URL https://security.microsoft.com/alerts?tid=875c82ee-30d3-4df1-a2c9-b97afafba73c.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### ***Task 3 Summary***

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

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

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

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

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

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

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

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

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### TASK 4: REVIEW AND MANAGE AUDIT LOGS

#### 4.1: Enable auditing in the Microsoft 365 Compliance Center

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

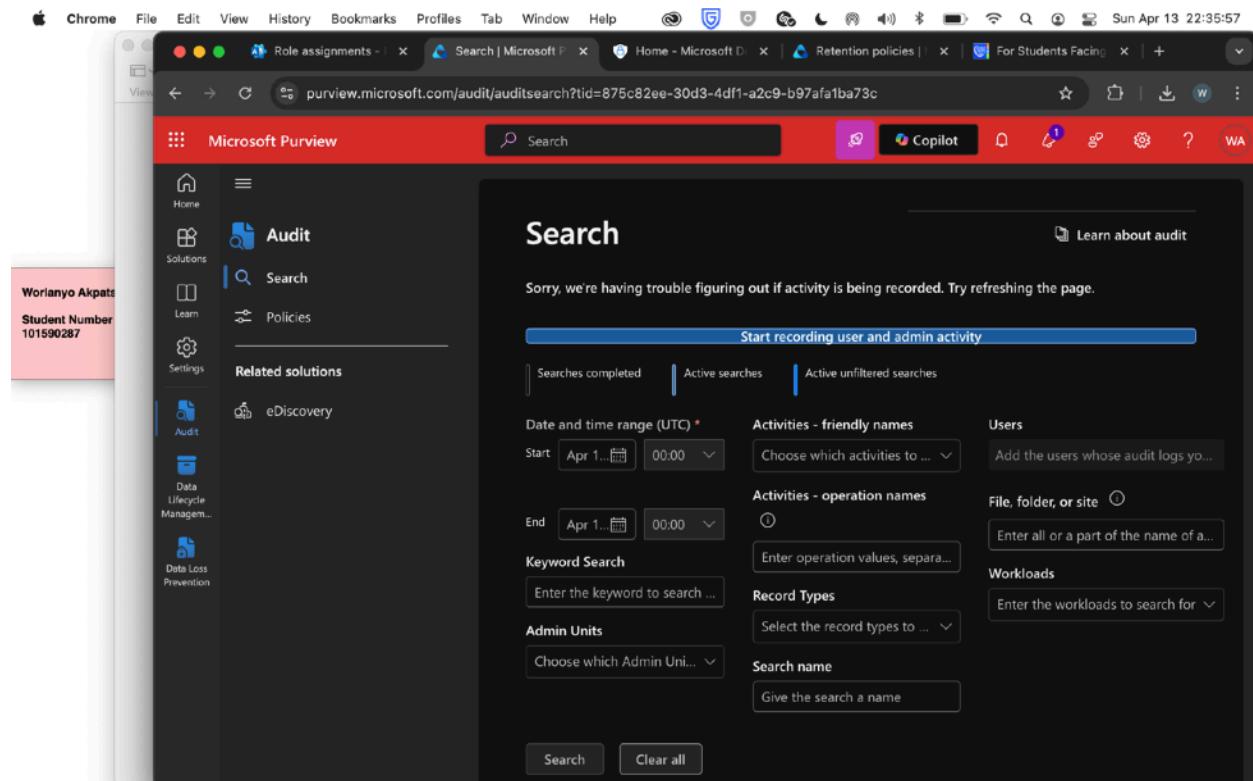
The screenshot shows a web browser window with multiple tabs open. The active tab is 'purview.microsoft.com/home?tid=875c82ee-30d3-4df1-a2c9-b97afa1ba73c'. The page has a dark theme with a sidebar on the left containing user information (Worlanyo Akpatsa, Student Number 101590287) and navigation links for Home, Solutions, Learn, Settings, Data Lifecycle Management, and Data Loss Prevention. The main content area displays the Microsoft Purview portal logo and a message about bringing solutions across data, identity, and compliance. A sidebar on the right lists various solutions: Audit, Communication Compliance, Compliance alerts, Compliance Manager, Data Catalog, Data Lifecycle Management, Data Loss Prevention, DSPM for AI, eDiscovery, Information Barriers, Information Protection, Insider Risk Management, and Records Management. A tooltip at the bottom right indicates that some features have moved or been retired.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Enabling Auditing by clicking ‘start recording user and admin activity’



The screenshot shows a Microsoft Purview Audit search interface. On the left, there's a sidebar with navigation links: Home, Solutions (Audit selected), Learn, Policies, Related solutions (eDiscovery), Audit, Data Lifecycle Management..., and Data Loss Prevention. The main area has a red header bar with the title 'Search'. Below it, a message says 'Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page.' A prominent blue button labeled 'Start recording user and admin activity' is centered. The search form includes fields for Date and time range (UTC), Activities - friendly names, Users, Activities - operation names, File, folder, or site, Keyword Search, Record Types, Workloads, Admin Units, and Search name. At the bottom are 'Search' and 'Clear all' buttons.

**Microsoft 365 Identity and Services – Enterprise Administration**

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

```
Terminal Shell Edit View Window Help Sun Apr 13 23:03:17

○ ● ● world — git> bash -c '#!/bin/bash012# We don't need return codes for "$(command)", only stdout is needed.012# Allow `[[ -n "$command" ]]`', `func "$command...
=> The following new directories will be created:
/usr/local/etc
/usr/local/include
/usr/local/lib
/usr/local/sbin
/usr/local/var
/usr/local/op
/usr/local/share/zsh
/usr/local/share/zsh/site-functions
/usr/local/var/homebrew
/usr/local/var/homebrew/linked
/usr/local/Cellar
/usr/local/Caskroom
/usr/local/Frameworks
=> The Xcode Command Line Tools will be installed.

Worlano Akpati: Press RETURN/ENTER to continue or any other key to abort:
Student Number: 101590287
=> /usr/bin/sudo /bin/chmod u=rwx /usr/local/bin /usr/local/share /usr/local/share/man /usr/local/share/man/man1
=> /usr/bin/sudo /bin/chmod g=rwx /usr/local/bin /usr/local/share /usr/local/share/man /usr/local/share/man/man1
=> /usr/bin/sudo /usr/sbin/chown worla /usr/local/bin /usr/local/share /usr/local/share/man /usr/local/share/man/man1
=> /usr/bin/sudo /usr/bin/chgrp admin /usr/local/bin /usr/local/share /usr/local/share/man /usr/local/share/man/man1
=> /usr/bin/sudo /bin/mkdir -p /usr/local/etc /usr/local/include /usr/local/lib /usr/local/sbin /usr/local/var /usr/local/opt /usr/local/share/zsh /usr/local/share/zsh/site-functions /usr/local/var/homebrew /usr/local/var/homebrew/linked /usr/local/Cellar /usr/local/Caskroom /usr/local/Frameworks
=> /usr/bin/sudo /bin/chmod u=rwx /usr/local/etc /usr/local/include /usr/local/lib /usr/local/sbin /usr/local/var /usr/local/opt /usr/local/share/zsh /usr/local/share/zsh/site-functions /usr/local/var/homebrew /usr/local/share/zsh /usr/local/share/zsh/site-functions
=> /usr/bin/sudo /bin/chmod go-w /usr/local/share/zsh /usr/local/share/zsh/site-functions
=> /usr/bin/sudo /usr/sbin/chown worla /usr/local/etc /usr/local/include /usr/local/lib /usr/local/sbin /usr/local/var /usr/local/opt /usr/local/share/zsh /usr/local/share/zsh/site-functions /usr/local/var/homebrew /usr/local/var/homebrew/linked /usr/local/Cellar /usr/local/Caskroom /usr/local/Frameworks
=> /usr/bin/sudo /usr/bin/chgrp admin /usr/local/etc /usr/local/include /usr/local/lib /usr/local/sbin /usr/local/var /usr/local/opt /usr/local/share/zsh /usr/local/share/zsh/site-functions /usr/local/var/homebrew /usr/local/var/homebrew/linked /usr/local/Cellar /usr/local/Caskroom /usr/local/Frameworks
=> /usr/bin/sudo /bin/mkdir -p /usr/local/Homebrew
=> /usr/bin/sudo /usr/sbin/chown -R worla:admin /usr/local/Homebrew
=> /usr/bin/sudo /bin/mkdir -p /Users/worla/Library/Caches/Homebrew
=> /usr/bin/sudo /bin/chmod g=rwx /Users/worla/Library/Caches/Homebrew
=> /usr/bin/sudo /usr/sbin/chown -R worla /Users/worla/Library/Caches/Homebrew
=> Searching online for the Command Line Tools
=> /usr/bin/sudo /usr/bin/touch /tmp/.com.apple.dt.CommandLineTools.installondemand.in-progress
=> Installing Command Line Tools for Xcode-13.2
=> /usr/bin/sudo /usr/sbin/softwareupdate -i Command Line Tools\ for\ Xcode-13.2
Software Update Tool

Finding available software

Downloading Command Line Tools for Xcode
Downloaded Command Line Tools for Xcode
Installing Command Line Tools for Xcode
Done with Command Line Tools for Xcode
Done.
=> /usr/bin/sudo /usr/bin/xcode-select --switch /Library/Developer/CommandLineTools
=> /usr/bin/sudo /bin/rm -f /tmp/.com.apple.dt.CommandLineTools.installondemand.in-progress
=> Downloading and installing Homebrew...
```

**Microsoft 365 Identity and Services – Enterprise Administration**

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

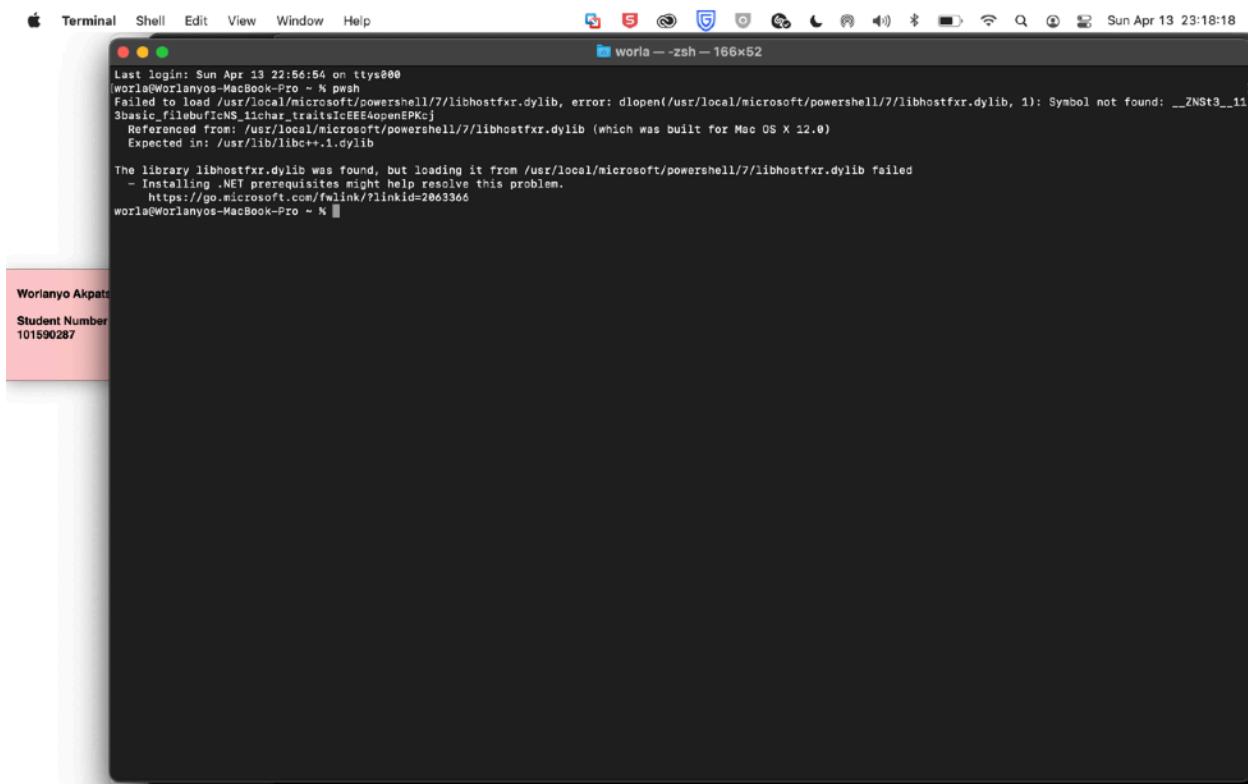
## D: Downloading and Installing powershell on Mac using terminal

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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



The screenshot shows a macOS Terminal window titled "worla -- zsh -- 166x52". The window contains the following text:

```
Last Login: Sun Apr 13 22:56:54 on ttys000
[worla@Worlanyos-MacBook-Pro ~] pwsh
Failed to load /usr/local/microsoft/powershell/7/libhostfxr.dylib, error: dlopen(/usr/local/microsoft/powershell/7/libhostfxr.dylib, 1): Symbol not found: __ZNSt3__11basic_filebufNS_11char_traitsIcEE4openSPMKj
Referenced from: /usr/local/microsoft/powershell/7/libhostfxr.dylib (which was built for Mac OS X 12.0)
Expected in: /usr/lib/libc++.1.dylib

The library libhostfxr.dylib was found, but loading it from /usr/local/microsoft/powershell/7/libhostfxr.dylib failed
- Installing .NET prerequisites might help resolve this problem.
  https://go.microsoft.com/fwlink/?LinkId=2063366
[worla@Worlanyos-MacBook-Pro ~] █
```

In the top-left corner of the terminal window, there is a small red box containing the student information:

Worlanyo Akpatsa  
Student Number  
101590287

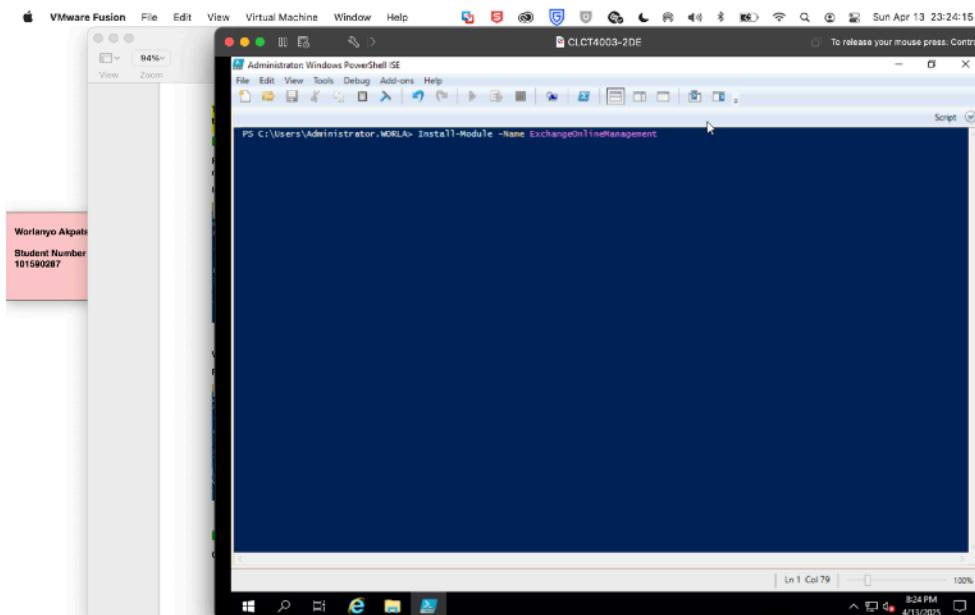
The process of running powershell on my mac was absolutely not working as the hardware is quite old so I decided to continue the steps of Auditing Log reviews on powershell using a VM.

## Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

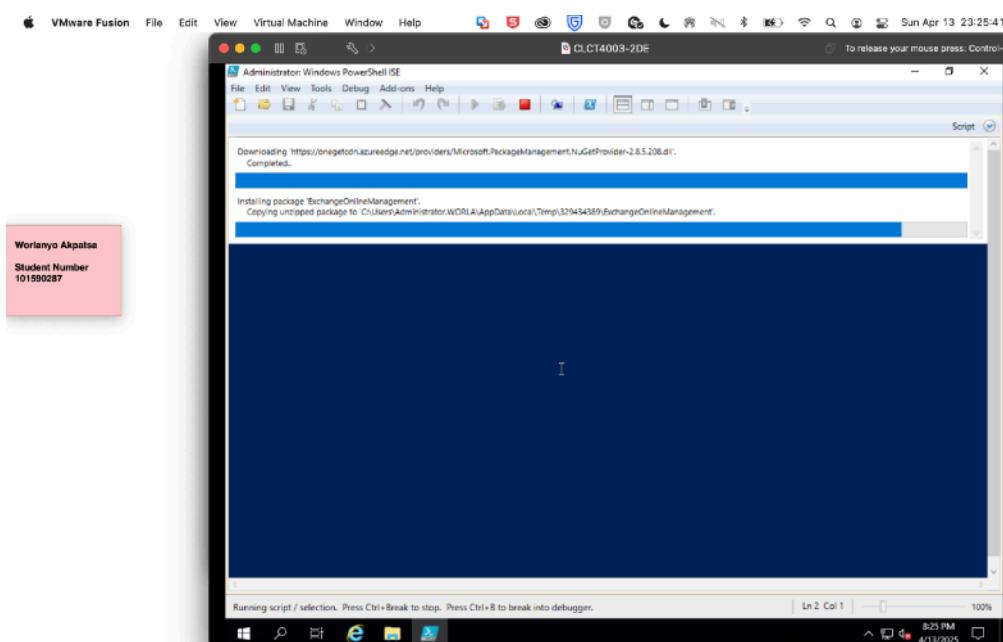
Term: Winter 2025

### A: Installing Exchange Online Module



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Help
PS C:\Users\Administrator.WORLA> Install-Module -Name ExchangeOnlineManagement
The term 'Install-Module' is not recognized as the name of a cmdlet, function, script file, or oper
ation. Check the spelling of the name, or if a path was included, verify that the path is correct
and try again.

At line:1 char:1
+ Install-Module -Name ExchangeOnlineManagement
+ ~~~~~~
```



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Help
PS C:\Users\Administrator.WORLA> Install-Module -Name ExchangeOnlineManagement
Downloading 'https://onegetcdn.azureedge.net/providers/Microsoft.PackageManagement.NuGetProvider-2.8.5.206.dll'.
Completed.

Installing package 'ExchangeOnlineManagement'.
Copying unzipped package to 'C:\Users\Administrator.WORLA\AppData\Local\Temp\339434389\ExchangeOnlineManagement'.
```

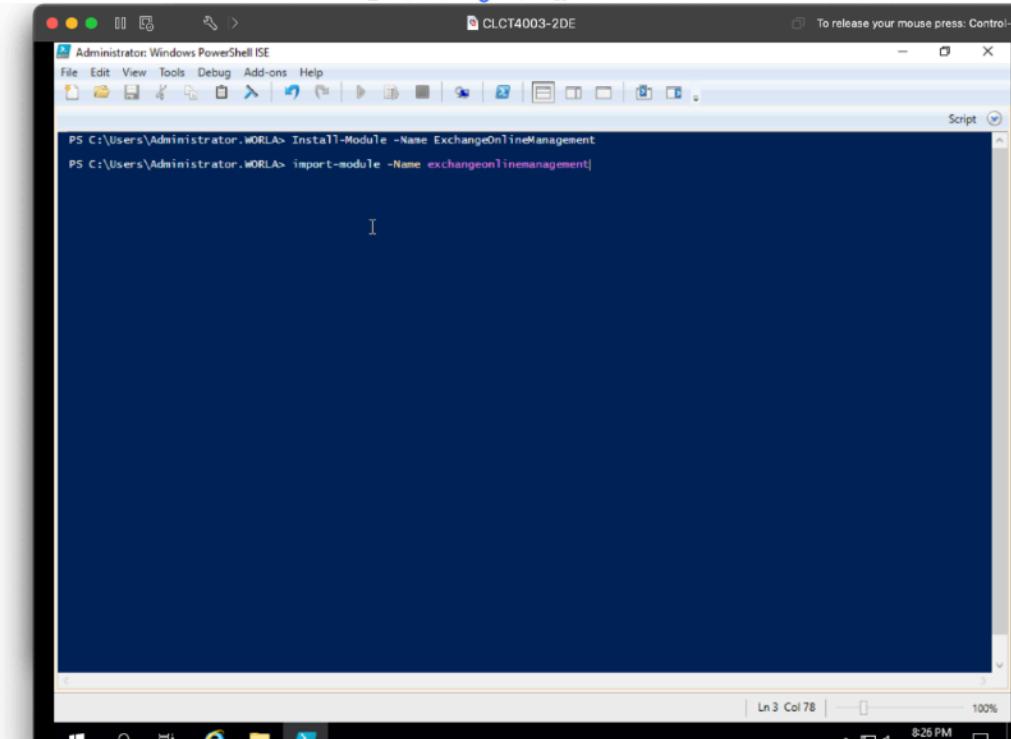
## Microsoft 365 Identity and Services – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: Importing Module



The screenshot shows a VMware Fusion interface with a Windows 10 desktop. A PowerShell ISE window is open, titled 'Administrator: Windows PowerShell ISE'. The command 'Install-Module -Name ExchangeOnlineManagement' is entered, followed by 'Import-Module -Name ExchangeOnlineManagement'. The PowerShell window has a status bar at the bottom indicating 'Ln 3 Col 78' and '8:26 PM 4/13/2025'. A small red box in the bottom-left corner of the slide contains the student information: 'Worlanyo Akpatsa' and 'Student Number 101590287'.

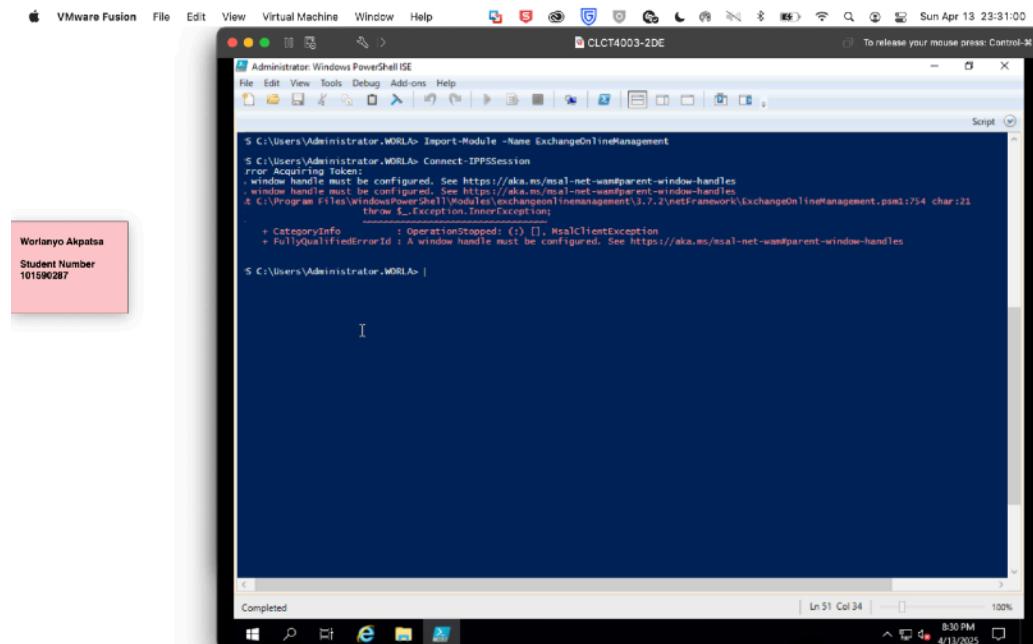
```
PS C:\Users\Administrator.WORLA> Install-Module -Name ExchangeOnlineManagement
PS C:\Users\Administrator.WORLA> import-module -Name ExchangeOnlineManagement
```

# Microsoft 365 Identity and Services – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

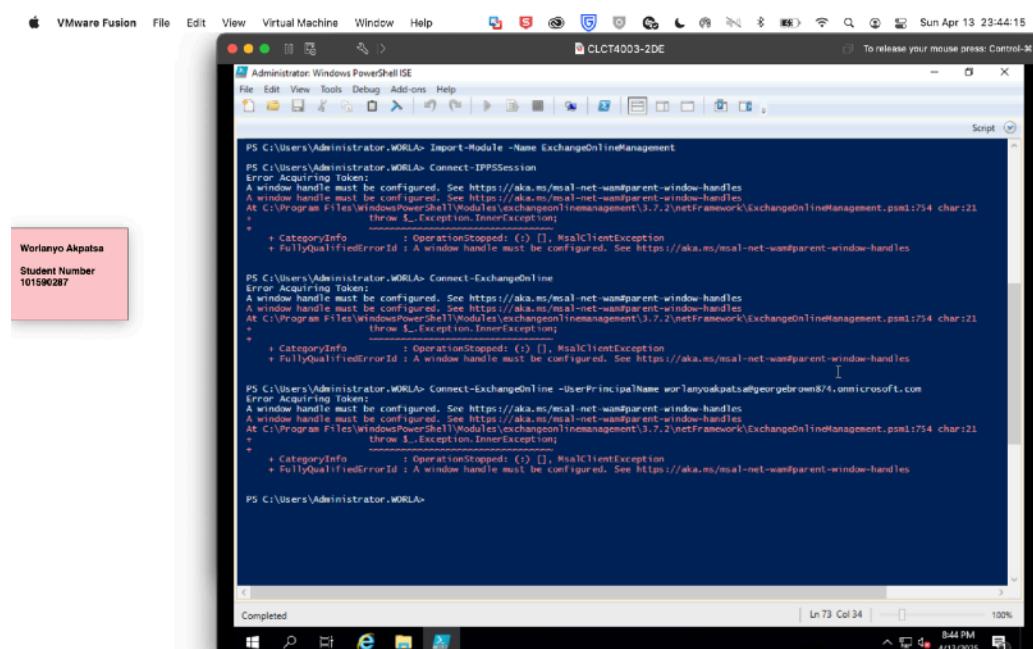
Term: Winter 2025

## C: Connecting to 365 Compliance Center



```
S C:\Users\Administrator.WORLA> Import-Module -Name ExchangeOnlineManagement
S C:\Users\Administrator.WORLA> Connect-IPSSession
Error Acquiring Token:
A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
At C:\Program Files\WindowsPowerShell\Modules\ExchangeOnlineManagement\3.7.2\NetFramework\ExchangeOnlineManagement.psm1:754 char:21
    + CategoryInfo          : OperationStopped: () [], MsalClientException
    + FullyQualifiedErrorId : A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles

S C:\Users\Administrator.WORLA>
```



```
PS C:\Users\Administrator.WORLA> Import-Module -Name ExchangeOnlineManagement
PS C:\Users\Administrator.WORLA> Connect-IPSSession
Error Acquiring Token:
A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
At C:\Program Files\WindowsPowerShell\Modules\ExchangeOnlineManagement\3.7.2\NetFramework\ExchangeOnlineManagement.psm1:754 char:21
    + CategoryInfo          : OperationStopped: () [], MsalClientException
    + FullyQualifiedErrorId : A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles

PS C:\Users\Administrator.WORLA> Connect-ExchangeOnline -UserPrincipalName worlanyoakpatsa@georgebrown.onmicrosoft.com
Error Acquiring Token:
A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
+ window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles
At C:\Program Files\WindowsPowerShell\Modules\ExchangeOnlineManagement\3.7.2\NetFramework\ExchangeOnlineManagement.psm1:754 char:21
    + CategoryInfo          : OperationStopped: () [], MsalClientException
    + FullyQualifiedErrorId : A window handle must be configured. See https://aka.ms/msal-net-wanparent-window-handles

PS C:\Users\Administrator.WORLA>
```

## **Microsoft 365 Identity and Services – Enterprise Administration**

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

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

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

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

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

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

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

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

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

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

## **Microsoft 365 Identity and Services – Enterprise Administration**

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

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

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

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

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

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