

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

---

### **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**

1. **Bulk Import Users:**
  - Use the Microsoft 365 admin center to bulk import 10 users from a CSV file.
  - Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users.
2. **Configure User Profiles:**
  - Ensure each user has a profile picture, contact information, and job title set.
  - Configure user settings to include organization-specific information.
3. **Create Office 365 Groups:**
  - Create three Office 365 groups for different departments: IT, HR, and Marketing.
  - Add users to their respective groups.
4. **Configure User Permissions:**
  - Assign specific permissions to the HR group to access sensitive HR documents in SharePoint.
  - Ensure the Marketing group has permission to create and manage Microsoft Teams.

##### **Task 2: Implementing Security Measures**

1. **Set Up and Configure Microsoft Defender for Office 365:**
  - Access the MS Defender and navigate to Secure Score.
  - Ensure that Safe Links and Safe Attachments have been enabled for all users.
  - Navigate to Policies and rules, then configure at least one policy to protect against phishing, malware, or spam.
2. **Set Up Data Encryption:**
  - Configure Microsoft 365 Message Encryption.

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

---

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

### **Task 3: Configuring and Managing Collaboration Tools**

#### **1. Set Up SharePoint Online:**

- Create an online SharePoint site for each department (IT, HR, Marketing).
- Configure document libraries and permissions for each site.
- Enable versioning and content approval for the HR document library.

#### **2. Implement OneDrive for Business:**

- Configure OneDrive settings to restrict external sharing.
- Enable file retention policies to ensure data is retained for at least five years.
- Set up a policy to automatically move old files to the Recycle Bin after a year.

#### **3. Set Up Viva Engage for Enterprise Social Networking:**

- Configure Viva to allow only internal communications.
- Set up groups for company-wide announcements and department-specific discussions.
- Ensure compliance with the company's social media policy.

### **Task 4: Monitoring and Reporting**

#### **1. Configure Audit Logs:**

- Enable and configure audit logging in the Microsoft 365 compliance center.
- Create a custom audit log search to track user activities related to at least one activity in SharePoint such as updating the site content.

#### **2. Set Up Alerts:**

- Configure alert policies to notify administrators of suspicious activities, such as multiple failed login attempts or mass deletion of files.
- Set up notifications for data loss prevention (DLP) policy breaches. (You can navigate to Insider risk management)

#### **3. Generate Usage Reports:**

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

---

### **4. Implement and Monitor Service Health:**

- Set up service health alerts to notify administrators of any issues with Microsoft 365 services.
- Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

#### **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

## Microsoft 365 Identity and Services – Enterprise Administration

---

### Task 1: Setting Up and Configuring User Accounts

#### 1.1 Bulk Import Users:

- Use the Microsoft 365 admin center to bulk import 10 users from a CSV file.

[ Screenshot: Downloaded sample blank CSV file from Microsoft Admin Center, in Active Users  
    > Add multiple Users ]

The screenshot shows a Microsoft Excel spreadsheet titled "Import\_User\_Template.csv". The spreadsheet contains 10 rows of data, each representing a user account. The columns are labeled: Username, First name, Last name, Display name, Job title, Department, Office number, and Office phone. The data is as follows:

|    | A                                 | B          | C         | D            | E               | F          | G             | H             |
|----|-----------------------------------|------------|-----------|--------------|-----------------|------------|---------------|---------------|
| 1  | Username                          | First name | Last name | Display name | Job title       | Department | Office number | Office phone  |
| 2  | user1@MSGSTUDENT.onmicrosoft.com  | User       | One       | User One     | Manager         | HR         | US            | Head Office   |
| 3  | user2@MSGSTUDENT.onmicrosoft.com  | User       | Two       | User Two     | Analyst         | IT         | US            | Main Office   |
| 4  | user3@MSGSTUDENT.onmicrosoft.com  | User       | Three     | User Three   | Team Lead       | Marketing  | US            | Branch Office |
| 5  | user4@MSGSTUDENT.onmicrosoft.com  | User       | Four      | User Four    | Developer       | IT         | US            | Main Office   |
| 6  | user5@MSGSTUDENT.onmicrosoft.com  | User       | Five      | User Five    | HR Specialist   | HR         | US            | Head Office   |
| 7  | user6@MSGSTUDENT.onmicrosoft.com  | User       | Six       | User Six     | Designer        | Marketing  | US            | Branch Office |
| 8  | user7@MSGSTUDENT.onmicrosoft.com  | User       | Seven     | User Seven   | IT Support      | IT         | US            | Main Office   |
| 9  | user8@MSGSTUDENT.onmicrosoft.com  | User       | Eight     | User Eight   | Project Manager | Marketing  | US            | Branch Office |
| 10 | user9@MSGSTUDENT.onmicrosoft.com  | User       | Nine      | User Nine    | Recruiter       | HR         | US            | Head Office   |
| 11 | user10@MSGSTUDENT.onmicrosoft.com | User       | Ten       | User Ten     | System Admin    | IT         | US            | Main Office   |
| 12 |                                   |            |           |              |                 |            |               |               |
| 13 |                                   |            |           |              |                 |            |               |               |
| 14 |                                   |            |           |              |                 |            |               |               |
| 15 |                                   |            |           |              |                 |            |               |               |
| 16 |                                   |            |           |              |                 |            |               |               |
| 17 |                                   |            |           |              |                 |            |               |               |
| 18 |                                   |            |           |              |                 |            |               |               |
| 19 |                                   |            |           |              |                 |            |               |               |
| 20 |                                   |            |           |              |                 |            |               |               |
| 21 |                                   |            |           |              |                 |            |               |               |
| 22 |                                   |            |           |              |                 |            |               |               |
| 23 |                                   |            |           |              |                 |            |               |               |

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with options like Home, Copilot, Users, Groups, Roles, Resources, Marketplace, Billing, Support, and Help & support. The main area is titled 'Active users > Add multiple users'. A flowchart indicates the process: Basics → Licenses → Finish. Under 'Basics', there are fields for First name, Last name, Username, and Domain (all set to MSGSTUDENT.onmicrosoft.com). There's also a checked checkbox for 'I'd like to upload a CSV with user information' and a 'Browse' button for 'Import\_User\_Template.csv'. Below this, there are links to download a blank CSV file or a CSV file with example user info. At the bottom are 'Next', 'Cancel', and a 'Help & support' link.

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

This screenshot continues the 'Add multiple users' wizard at the 'Licenses' step. The flowchart now shows 'Basics' → 'Licenses' → 'Finish'. In the 'Licenses' section, it says 'Select the location and product licenses for the 10 users you're adding.' A dropdown menu for 'Location' is set to 'Canada'. Below this, under 'Assign licenses', there's a checked checkbox for 'Microsoft 365 E3 (no Teams)' with the note '11 of 25 licenses available'. Other options shown are 'Microsoft 365 E5 (no Teams)' (unchecked, note: You're out of licenses), 'Microsoft Power Automate Free' (unchecked, note: 10000 of 10000 licenses available), and 'Don't assign any licenses (not recommended)'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with options like Home, Copilot, Users (Active users, Contacts, Guest users, Deleted users), Groups, Roles, Resources, Marketplace, Billing (Your products, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications, Cost Management), Support, and Help & support. The main content area is titled "Active users > Add multiple users". A flowchart on the left indicates the steps: Basics → Licenses → Finish. The "Review and finish adding multiple users" section shows "Users to add: 10 users" with an "Edit" link. It also shows "Licenses bought: None". Under "Licenses assigned", it lists "Location: Canada", "Licenses: Microsoft 365 E3 (no Teams)", and "Apps: Places Core, Graph Connectors Search with Index, Immersive spaces for Teams, 46 more" with an "Edit" link. At the bottom are "Back", "Add users" (highlighted in blue), and "Cancel" buttons.

This screenshot shows the same interface after the users have been added. The flowchart now has green checkmarks next to "Basics", "Licenses", and "Finish". A prominent message box 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." There are "Print" and "Download user details" buttons. A red box highlights a table listing the added users:

| Display name | Username                         |
|--------------|----------------------------------|
| User One     | user1@MSGSTUDENT.onmicrosoft.com |
| User Two     | user2@MSGSTUDENT.onmicrosoft.com |
| User Three   | user3@MSGSTUDENT.onmicrosoft.com |
| User Four    | user4@MSGSTUDENT.onmicrosoft.com |
| User Five    | user5@MSGSTUDENT.onmicrosoft.com |
| User Six     | user6@MSGSTUDENT.onmicrosoft.com |
| User Seven   | user7@MSGSTUDENT.onmicrosoft.com |

At the bottom are "Close" and "Help & support" buttons. The system status bar at the bottom right shows "Feels colder Now", a battery icon, and the date/time "10:29 PM 11-Dec-24".

## Microsoft 365 Identity and Services – Enterprise Administration

### 1.2 Configure User Profiles:

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

The screenshot shows the Microsoft 365 Admin Center interface. On the left, the navigation menu includes Home, Copilot, Users (Active users selected), Groups, Roles, Resources, Marketplace, Billing, Support, and Help & support. The main content area displays a list of users: Test1 user, User Eight, User Five, User Four, User Nine, User One (selected and highlighted with a red box), User Seven, User Six, User Ten, User Three, and User Two. The 'User One' card shows a profile picture of a woman, the name 'User One', and options to Reset password, Block sign-in, or Delete user. Below the card are tabs for Account (selected), Devices, Licenses and apps, Mail, and OneDrive. A note says: 'The alternate email address shouldn't use any domains associated with this tenant. For example, you could use a personal email address. Change the alternate address' with a link to 'Change the alternate address'. To the right, sections include Username and email (user1@MSGSTUDENT.onmicrosoft.com), Aliases (Manage username and email), Last sign-in (View last 30 days), Sign-out (Sign this user out of all Microsoft 365 sessions, Sign out of all sessions), Alternate email address (use\*\*\*\*\*@MSGSTUDENT.onmicrosoft.com), Groups (Manage groups), Roles (No administrator access, Manage roles), and Manager (None provided, Add manager). The status bar at the bottom shows the date and time as 10:37 PM, 11-Dec-24.

Configure user settings to include organization-specific information.

The screenshot shows the 'Manage contact information' dialog for 'User One'. The dialog has a header 'Manage contact information' with a back arrow. It contains fields for First name (User), Last name (One), Display name (User One), Job title (Manager), Department (HR), Office (US), Office phone (Head Office), and Fax number (123-456-7890). A 'Save changes' button is at the bottom. The background shows the same user list and navigation menu as the previous screenshot. The status bar at the bottom shows the date and time as 10:36 PM, 11-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various categories like Home, Copilot, Users, Groups, Roles, Resources, Marketplace, Billing, and Support. Under the 'Users' section, 'Active users' is selected, and a list of users is displayed, with 'User One' checked. The main content area is titled 'Manage contact information' and contains fields for Department (HR), Office (US), Office phone (Head Office), Fax number (123-456-7890), Mobile phone (P@ssw0rd123), Street address (123 Main Street), City (Toronto), State or province (ON), Zip or postal code (10001), and Country or region (CANADA). A red box highlights the entire form area. At the bottom right of the form is a 'Save changes' button.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is identical to the previous screenshot. In the main content area, it says 'Change photo' and displays a circular placeholder image of a person with a green background. Below the image is a 'Choose photo' button. The user list on the left shows 'User Two' checked. At the bottom right of the page is a 'Save changes' button.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, the navigation menu includes Home, Copilot, Users (Active users, Contacts, Guest users, Deleted users), Groups, Roles, Resources, Marketplace, Billing (Your products, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications, Cost Management), and Support. The main content area displays a user profile for "User Two". The profile card shows a green placeholder photo, the name "User Two", and three action buttons: "Reset password", "Block sign-in", and "Delete user". Below the card, there are tabs for Account, Devices, Licenses and apps, Mail, and OneDrive. Under the "Account" tab, there is a note about alternate email addresses. The "Username and email" section shows the email "user2@MSGSTUDENT.onmicrosoft.com" and a link to "Manage username and email". The "Aliases" section shows "MSGSTUDENT" and a link to "Manage groups". The "Last sign-in" section shows "View last 30 days". The "Sign-out" section allows signing out of all Microsoft 365 sessions. The "Alternate email address" section shows "use\*\*\*\*\*@MSGSTUDENT.onmicrosoft.com" and a link to "Edit address". The "Groups" section shows "Manager" and "None provided". The "Roles" section shows "No administrator access" and a link to "Manage roles". The bottom right corner of the screen shows system status: 1°C, Partly cloudy, 10:40 PM, 11-Dec-24.

This screenshot shows the "Manage contact information" form for "User Two". The form fields are as follows: First name (User), Last name (Two), Display name \* (User Two), Job title (Analyst), Department (IT), Office (US), Office phone (Main Office), and Fax number (234-567-8901). A "Save changes" button is at the bottom. The rest of the page is identical to the first screenshot, showing the user list and navigation menu.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various options like Home, Copilot, Users, Groups, Roles, Resources, Marketplace, Billing, Support, and Help & support. In the center, a search bar is at the top, followed by a list of users: Test1 user, User Eight, User Five, User Four, User Nine, User One, User Seven, User Six, User Ten, User Three, and User Two. User Two is selected and highlighted with a blue checkmark. A red box highlights the 'Manage contact information' dialog box. This dialog contains fields for Department (IT), Office (US), Office phone (Main Office), Fax number (234-567-8901), Mobile phone (P@ssw0rd123), Street address (456 Elm Street), City (Mississauga), State or province (ON), Zip or postal code (94103), Country or region (CANADA). At the bottom right of the dialog is a 'Save changes' button.

### 1.3 Create Office 365 Groups:

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

The screenshot shows the 'Review and finish adding group' page. On the left, there's a sidebar with a checklist: Basics (checked), Owners (checked), Members (checked), Settings (checked), and Finish (unchecked). The main area shows the 'Review and finish adding group' section with the following details:

- Basics**: Name: IT, Description: This group is for IT team. A red box highlights this section.
- Owners**: Shivani Varu. A red box highlights this section.
- Members**: User Five, User One, User Seven, User Three. A red box highlights this section.
- Settings**: Email: itteam@MSGSTUDENT.onmicrosoft.com, Privacy: Private, Role assignment: Disabled. A red box highlights this section.

At the bottom, there are 'Back' and 'Create group' buttons, and a 'Cancel' button on the right. The status bar at the bottom shows system information: 1°C Partly cloudy, 10:45 PM, 11-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. A success message 'IT group created' is displayed in a red-bordered box. The navigation pane on the left shows a progress bar with steps: Basics (checkmark), Owners (checkmark), Members (checkmark), Settings (checkmark), and Finish (checkmark). The main content area includes a note that the group will appear in 5 minutes, a list of what can be done with the group, and links for more information and next steps.

The screenshot shows the 'Review and finish adding group' step in the Microsoft 365 Admin Center. It displays the summary of the group settings: Group type (Microsoft 365), Basics (Name: HR, Description: This group is for HR team), Owners (Shivani Varu), Members (User Four, User Six, User Two), and Settings (Email: hrteam@MSGSTUDENT.onmicrosoft.com, Privacy: Private, Role assignment: Disabled). The 'Create group' button is visible at the bottom.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a sidebar lists navigation options: Home, Active groups, Add a Microsoft 365 group, Groups, People, Devices, Reports, and Settings. The 'Add a Microsoft 365 group' option is selected. The main content area displays a progress bar with five steps: Basics (checkmark), Owners (checkmark), Members (checkmark), Settings (checkmark), and Finish (blue circle). A prominent green checkmark icon with the text 'HR group created' is centered in a red-bordered box. Below it, a message states: 'HR group will appear in your list of Active groups within 5 minutes.' A list of three settings is provided: 'Send copies of group conversations and events to group members' inboxes', 'Let people outside the organization email this group', and 'Hide from my organization's global address list'. A section titled 'Would you like to know more?' includes a link to 'Using groups to collaborate effectively'. A 'Next steps' section suggests 'Add another Microsoft 365 (recommended) group'. At the bottom right is a 'Close' button. The taskbar at the bottom shows various application icons and the system clock.

The screenshot shows the 'Review and finish adding group' step in the Microsoft 365 Admin Center. The sidebar and navigation bar are identical to the previous screenshot. The main content area is titled 'Review and finish adding group' and contains a message: 'You're almost there - make sure everything looks right before adding your new group.' Below this, a 'Group type' section shows 'Microsoft 365' with an 'Edit' link. Three sections are displayed in boxes: 'Basics' (Name: Marketing, Description: This group is for marketing team, Edit link); 'Owners' (Shivani Varu, Edit link); and 'Members' (User Eight, User Nine, User Ten, Edit link). A fourth section, 'Settings' (Email: marketingteam@MSGSTUDENT.onmicrosoft.com, Privacy: Private, Role assignment: Disabled), is also shown with an edit link. At the bottom are 'Back', 'Create group', and 'Cancel' buttons. The taskbar at the bottom shows various application icons and the system clock.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a sidebar lists steps: Basics, Owners, Members, Settings, and Finish. A red box highlights the 'Marketing group created' message at the top right. Below it, a note says 'Marketing group will appear in your list of Active groups within 5 minutes.' A list of settings follows, and links for 'Would you like to know more?' and 'Next steps' are provided.

The screenshot shows the Microsoft 365 Admin Center interface with the 'Active groups' page selected in the sidebar. A red box highlights the 'Active groups' section. The main area displays a table of groups, with a red box highlighting the 'Marketing' group row. The table columns include Name, Email, Sync status, Membership type, Privacy, and Created on.

| Name ↑      | Email                                    | Sync status | Membership type | Privacy | Created on                    |
|-------------|------------------------------------------|-------------|-----------------|---------|-------------------------------|
| All Company | allcompany@MSGSTUDENT.onmicrosoft.com    | Synced      | Assigned        | Public  | November 14, 2024 at 12:28 AM |
| HR          | hrtteam@MSGSTUDENT.onmicrosoft.com       | Synced      | Assigned        | Private | December 12, 2024 at 3:49 AM  |
| IT          | itteam@MSGSTUDENT.onmicrosoft.com        | Synced      | Assigned        | Private | December 12, 2024 at 3:46 AM  |
| Marketing   | marketingteam@MSGSTUDENT.onmicrosoft.com | Synced      | Assigned        | Private | December 12, 2024 at 3:51 AM  |

## Microsoft 365 Identity and Services – Enterprise Administration

Add users to their respective groups.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, the navigation menu is visible with the 'Groups' section expanded, showing 'Active groups'. In the main content area, the 'Active groups' page is displayed. A specific group named 'IT' is selected and highlighted with a red box. The 'Membership' tab is active. The 'Members' section shows a list of users with checkboxes next to their names. Another red box highlights this list. The users listed are:

| Name       | Email address                    |
|------------|----------------------------------|
| User Five  | user5@MSGSTUDENT.onmicrosoft.com |
| User One   | user1@MSGSTUDENT.onmicrosoft.com |
| User Seven | user7@MSGSTUDENT.onmicrosoft.com |
| User Three | user3@MSGSTUDENT.onmicrosoft.com |

The screenshot shows the Microsoft 365 Admin Center interface, similar to the previous one but for the 'HR' group. The 'HR' group is selected and highlighted with a red box. The 'Membership' tab is active, and the 'Members' section shows a list of users with checkboxes. Another red box highlights this list. The users listed are:

| Name      | Email address                    |
|-----------|----------------------------------|
| User Four | user4@MSGSTUDENT.onmicrosoft.com |
| User Six  | user6@MSGSTUDENT.onmicrosoft.com |
| User Two  | user2@MSGSTUDENT.onmicrosoft.com |

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various options like Home, Copilot, Users, Groups, Roles, Resources, Marketplace, and Billing. Under Groups, 'Active groups' is selected. In the main content area, the 'Active groups' page is displayed. A specific group, 'Marketing', is highlighted with a red box. This group is described as a 'Private group'. Below the group card, there are tabs for General, Membership (which is selected), and Settings. The 'Membership' tab shows a table with columns for Name and Email address. Three users are listed: User Eight (user8@MSGSTUDENT.onmicrosoft.com), User Nine (user9@MSGSTUDENT.onmicrosoft.com), and User Ten (user10@MSGSTUDENT.onmicrosoft.com). Each user has a small profile icon next to their name.

### 1.4 Configure User Permissions:

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

The screenshot shows a SharePoint site titled 'HR Document - Home'. The left navigation bar includes links for Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area features a news section with a tablet icon and a 'Keep your team updated with news on your team site' message. On the right, there's a 'Group membership' section with a green button for 'Add members'. It lists four members: User Two (Member), User Four (Member), User Six (Owner), and Shivani Varu (Owner). The bottom right corner shows a weather widget indicating 1°C and partly cloudy conditions.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the Microsoft SharePoint site 'HR Document - Home' at [msgstudent.sharepoint.com/sites/hrteam](https://msgstudent.sharepoint.com/sites/hrteam). The 'Permissions' section is highlighted with a red box. It shows Site owners - full control for 'HR Document Members' and Site visitors - no control for 'None'. Other sections like Site members - limited control and Site sharing are also visible.

This screenshot shows the Microsoft SharePoint site 'HR Document - Home' at [msgstudent.sharepoint.com/sites/hrteam](https://msgstudent.sharepoint.com/sites/hrteam). The 'Site sharing settings' section is highlighted with a red box. It includes options for Sharing permissions (Site owners and members can share files, folders, and the site), Access requests (allow access requests for HR Document Owners or Specific email), and a message for the request access page. A note says 'Please allow up to three business days for us to review your request. For urgent matters, contact hr@msgstudent.onmicrosoft.com.' Buttons for Save and Discard are at the bottom right.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the SharePoint admin center interface. On the left, the navigation menu includes 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 area is titled "Active sites" and displays a list of sites. One site, "HR Document", is highlighted with a red box. Its details are shown in a card: "HD" icon, "HR Document" name, "Private group", and buttons for Email, View site, and Delete. Below the card, it says "This group is for HR team". Under "Settings", there are tabs for General, Activity, Membership, and Settings (selected). In the "Email" section, a checkbox for "Send copies of team emails and events to team members' inboxes" is checked and highlighted with a red box. In the "Privacy" section, a radio button for "Private" is selected and highlighted with a red box. In the "External file sharing" section, a dropdown menu set to "Only people in your organization" is highlighted with a red box. At the bottom right, there is a "Save" button.

The screenshot shows the SharePoint permissions page for a document library. The top navigation bar includes All admin centers - Microsoft 365, Permissions: Documents, and Incognito (2). The left sidebar lists Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle Bin, and EDIT LINKS. The main content area has tabs for BROWSE and PERMISSIONS (selected). Under PERMISSIONS, there are buttons for Delete unique permissions inheritance, Grant Permissions, Edit User Permissions, Remove User Permissions, Check Permissions, and Check. A warning message "⚠ This library has unique permissions." is displayed. Below this, a table shows permission details:

|                                     | Type             | Permission Levels |
|-------------------------------------|------------------|-------------------|
| <input type="checkbox"/> Name       | SharePoint Group | Edit              |
| <input type="checkbox"/> HR Members | SharePoint Group | Full Control      |
| <input type="checkbox"/> HR Owners  |                  |                   |

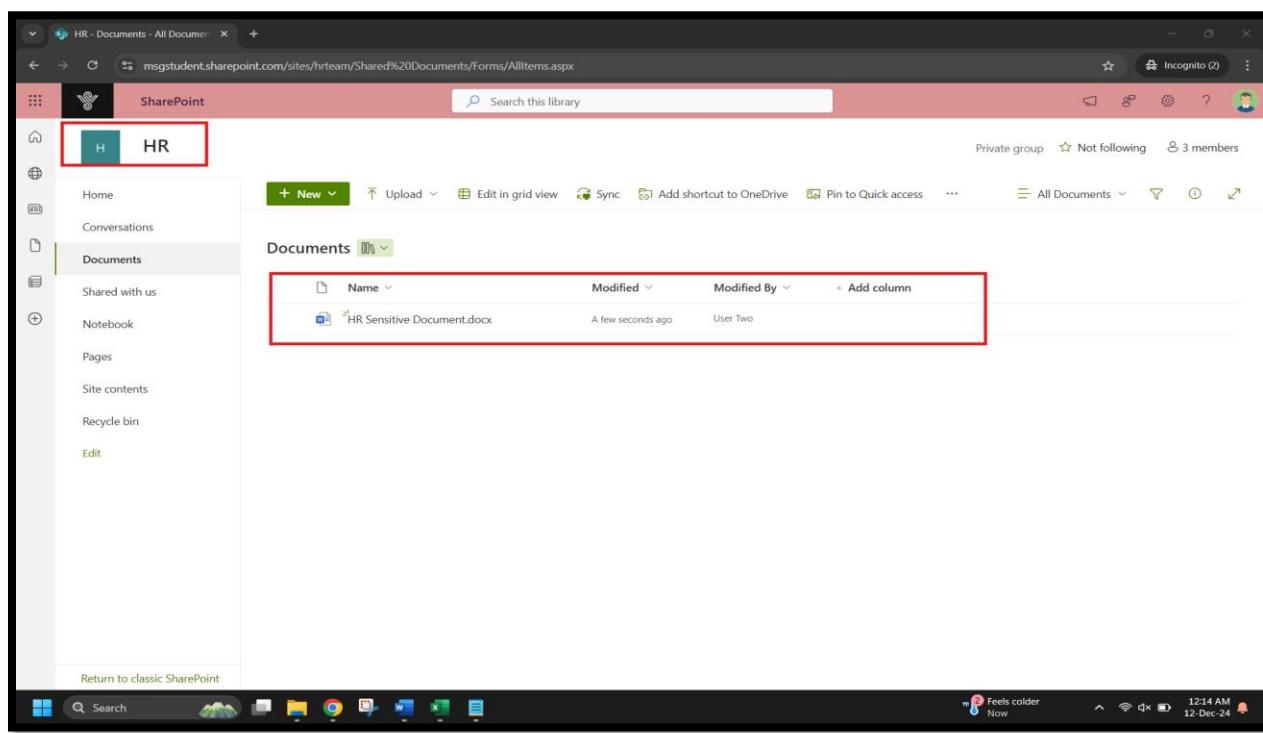
## Microsoft 365 Identity and Services – Enterprise Administration

[ Screenshot: It's confirmed that other users( here User 8, which does not belongs to HR) are not allowed to do anything with HR sensitive Document ]

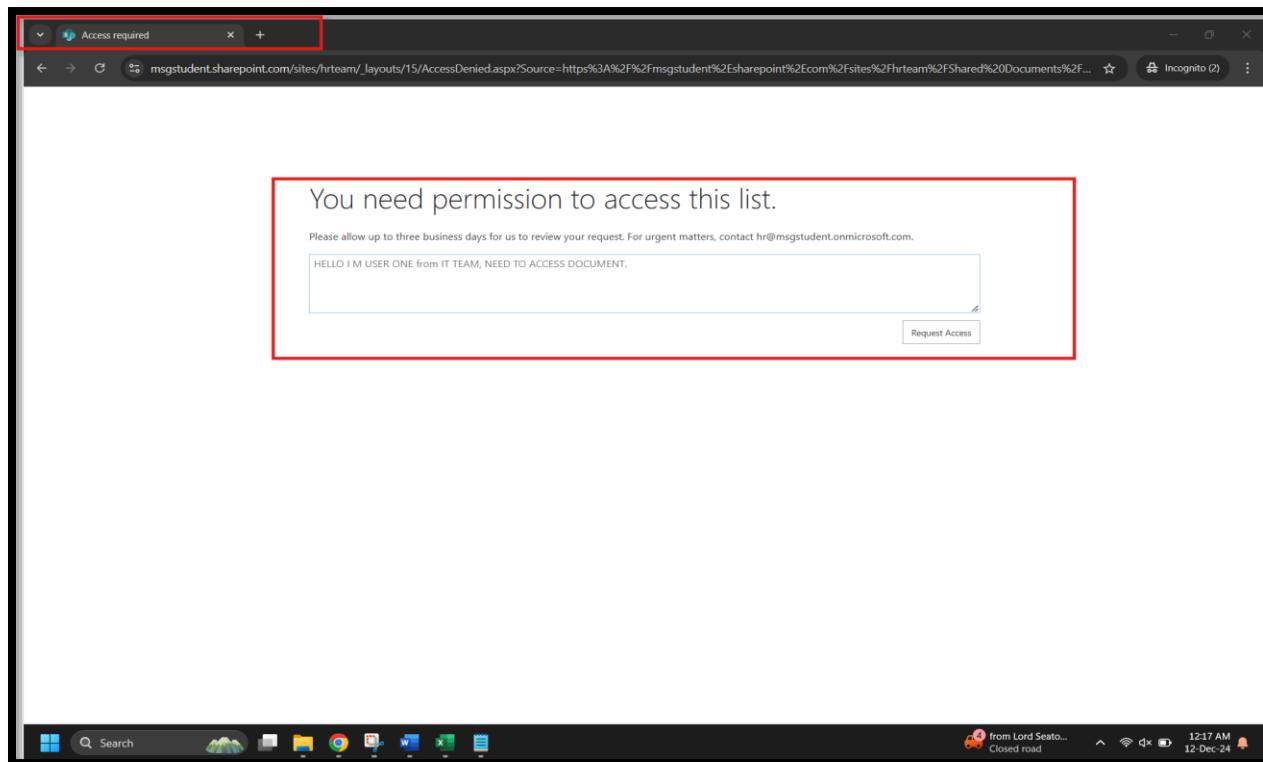
This screenshot shows the 'Permissions: Documents' page in SharePoint. The left navigation bar includes Home, Conversations, Documents, Notebook, Pages, Site contents, and Recycle Bin. The main area displays a warning message: 'This library has unique permissions.' Below this, there are sections for 'Delete unique permissions', 'Grant Permissions', 'Edit User Permissions', 'Remove User Permissions', and 'Check Permissions'. A 'Check Permissions' dialog box is open, showing 'User/Group: User Eight x'. The message inside the dialog states: 'The user will not be able to browse to the list. The user may need to be granted access to the containing site. Permission levels given to User Eight (i09fjmembership\user@msgstudent.onmicrosoft.com)' followed by 'None'. At the bottom right of the dialog are 'Check Now' and 'Close' buttons.

This screenshot shows a Microsoft Word document titled 'Document.docx'. The document contains the text 'XXX THIS IS HR SPECIFIC SENSITIVE DOCUMENT XXX' and '- - Created by USER TWO (HR Manager)'. In the top right corner of the Word interface, a sidebar displays the user profile 'MSGSTUDENT' and the name 'User Two'. The sidebar also includes options for 'View account' and 'My Microsoft 365 profile'. The Word ribbon tabs at the top include File, Home, Insert, Layout, References, Review, View, and Help. The status bar at the bottom shows 'Page 1 of 1 18 words English (U.S.) Text Predictions: On Editor Suggestions: Showing'. The taskbar at the very bottom of the screen shows various pinned icons.

## Microsoft 365 Identity and Services – Enterprise Administration



[ Screenshot: User one ( belongs to IT Team ) trying to access HR specific Document which is not allowed by HR team ]



## Microsoft 365 Identity and Services – Enterprise Administration

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

The screenshot shows the Microsoft Teams admin center interface. On the left, there's a navigation sidebar with various options like Dashboard, Teams, Manage teams, etc. The main area is titled 'Manage teams' and displays a 'Users summary' with 17 total users, 17 internal users, and 0 guests. A 'Quick guide to the new chats, teams and channels experience' is visible. On the right, a modal window titled 'Add a new team' is open. It contains fields for 'Name' (Marketing Team), 'Description' (This is TechSolutions Inc's Marketing Team), 'Team owners' (Shivani Varu), and 'Privacy' (Private). The 'Apply' button is at the bottom right of the modal.

The screenshot shows the Microsoft Teams admin center interface, specifically for the 'Marketing Team'. The team details are shown on the left, including the team name, a profile picture, and member information. On the right, a modal window titled 'Add members' is open. It includes a search bar for 'user' and a list titled 'Team members to add: 3' containing three users: 'User Nine (USER9) RECRUITER', 'User Eight (USER8) PROJECT MANAGER', and 'User Ten (USER10) SYSTEM ADMIN'. The 'Apply' button is at the bottom right of the modal.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Teams admin center interface. On the left, a navigation sidebar lists various team management options like Dashboard, Teams, Users, etc. The main area displays the 'Marketing Team' details, which are highlighted with a red box. It includes the team's name, a brief description ('This is TechSolutions Inc's Marketing Team'), a purple square icon with 'MT', a list of team members (Shivani Varu, User Eight, User Nine, User Ten), and privacy settings (Private). Below this, another red box highlights the 'Members' tab of the team's settings page, showing a table of team members with columns for Display name, Username, Title, Location, and Role.

| Display name | Username               | Title           | Location | Role   |
|--------------|------------------------|-----------------|----------|--------|
| SV           | ShivaniVaru@MSGSTUD... | -               | -        | Owner  |
| UE           | User Eight             | Project Manager | Canada   | Member |
| UN           | User Nine              | Team Lead       | Canada   | Member |
| UT           | User Ten               | Designer        | Canada   | Member |

The screenshot shows the 'Settings' page for the Marketing Team, also highlighted with a red box. The 'General' section shows the team's name (Marketing Team), description ('This is TechSolutions Inc's Marketing Team'), and privacy settings (Private). The 'Member permissions' section, also highlighted with a red box, lists several permissions for team members: Edit sent messages (On), Delete sent messages (On), Add and edit channels (On), Delete channels (On), Add, edit, or remove tabs (On), Add, edit, or remove connectors (On), and Add, edit, or remove apps (On). Other sections visible include 'Mentions' and 'Guest permissions'.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is collapsed, showing navigation links for Home, Copilot, Users (Active users, Contacts, Guest users, Deleted users), Groups (Active groups, Deleted groups, Shared mailboxes), Roles, Resources, Marketplace, and Billing. The main content area is titled "Active groups" and displays the "Marketing Team" under "Microsoft 365 groups". The "Settings" tab is selected. The Marketing Team is described as a "Private team". It has a blue icon with "MT". Action buttons include Email, Open in Teams, View site, and Delete. Below the description, there are sections for "Email", "Privacy", "External file sharing", "Sensitivity label", "Teams channels", and "Teams conversations". Under "Email", there are checkboxes for letting people outside the organization email the team, sending copies of team emails and events to team members' inboxes, and not showing the team email address in Outlook. The "Privacy" section shows "Private" is selected. Under "External file sharing", it says "New and existing guests". Under "Sensitivity label", it says "None". Under "Teams channels", three checkboxes are checked: "Team members can add channels and edit existing channels", "Team members can add and edit private channels", and "Team members can delete channels". Under "Teams conversations", two checkboxes are checked: "Allow members to edit their sent messages" and "Allow members to delete their sent messages". The bottom right corner shows system status: 1°C, Mostly clear, 11:36 PM, 11-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

### Task 2: Implementing Security Measures

#### 2.1 Set Up and Configure Microsoft Defender for Office 365:

- Access the MS Defender and navigate to Secure Score.

The screenshot shows the Microsoft Secure Score dashboard. On the left, there's a navigation sidebar with various sections like Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, and more. The 'Secure score' option under 'Exposure insights' is highlighted with a red box. The main area is titled 'Microsoft Secure Score' and displays a summary of the organization's security posture. It shows a secure score of 41.78% (161.27/386 points achieved) with a bar chart showing progress from 1/1/16 to 12/11. Below this, there's a section for 'Actions to review' with a count of 56 items. A large red box highlights the user profile in the top right corner, which shows 'MSGSTUDENT' and 'Shivani Varu'. The bottom part of the dashboard lists 'Top recommended actions' with their respective details and scores.

| Recommended action                                                  | Score impact | Status                           | Category |
|---------------------------------------------------------------------|--------------|----------------------------------|----------|
| Ensure multifactor authentication is enabled for all users in ad... | +2.59%       | <input type="radio"/> To address | Identity |
| Enable Conditional Access policies to block legacy authentication   | +2.07%       | <input type="radio"/> To address | Identity |
| Ensure that intelligence for impersonation protection is enabled    | +2.07%       | <input type="radio"/> To address | Apps     |
| Move messages that are detected as impersonated users by ma...      | +2.07%       | <input type="radio"/> To address | Apps     |
| Enable impersonated domain protection                               | +2.07%       | <input type="radio"/> To address | Apps     |

## Microsoft 365 Identity and Services – Enterprise Administration

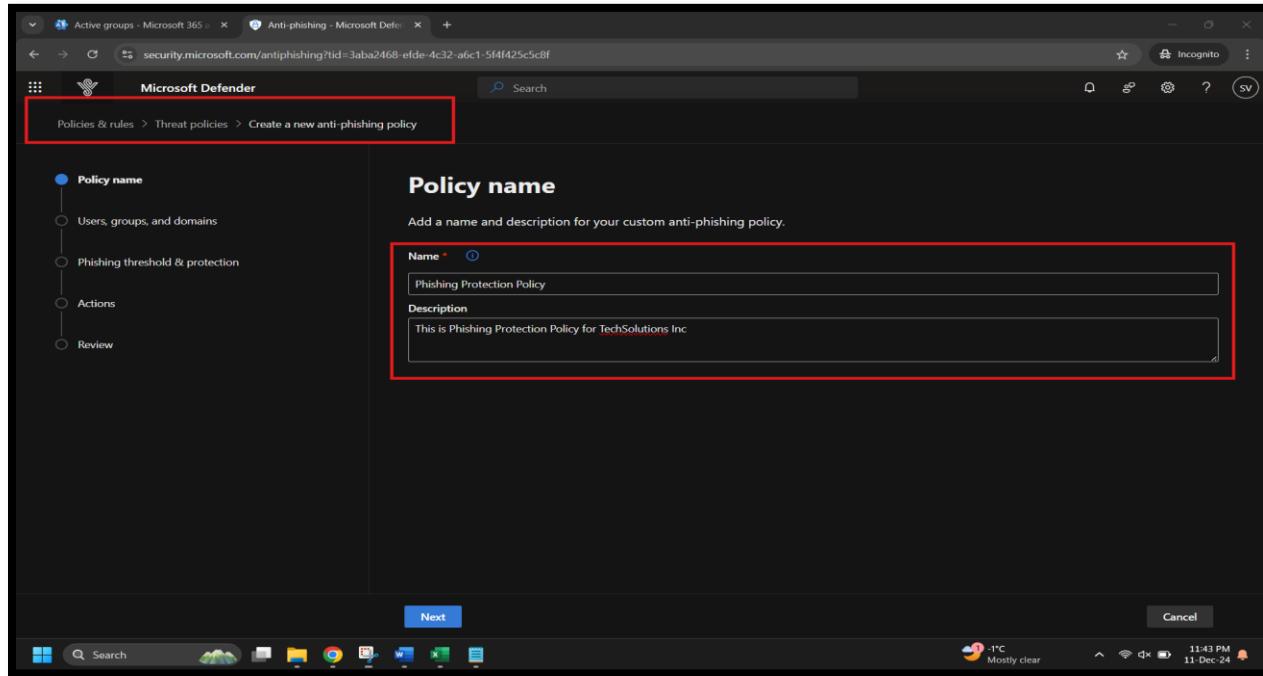
- Ensure that Safe Links and Safe Attachments have been enabled for all users.

The screenshot shows the Microsoft Defender Threat policies interface. The left sidebar includes sections for Active groups, 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, Governance log), and Policies. The main content area is titled "Safe links" and displays a table of threat policies. A single row is visible, labeled "Built-in protection (Microsoft)" with a status of "On" and priority "Lowest". The entire table row is highlighted with a red box.

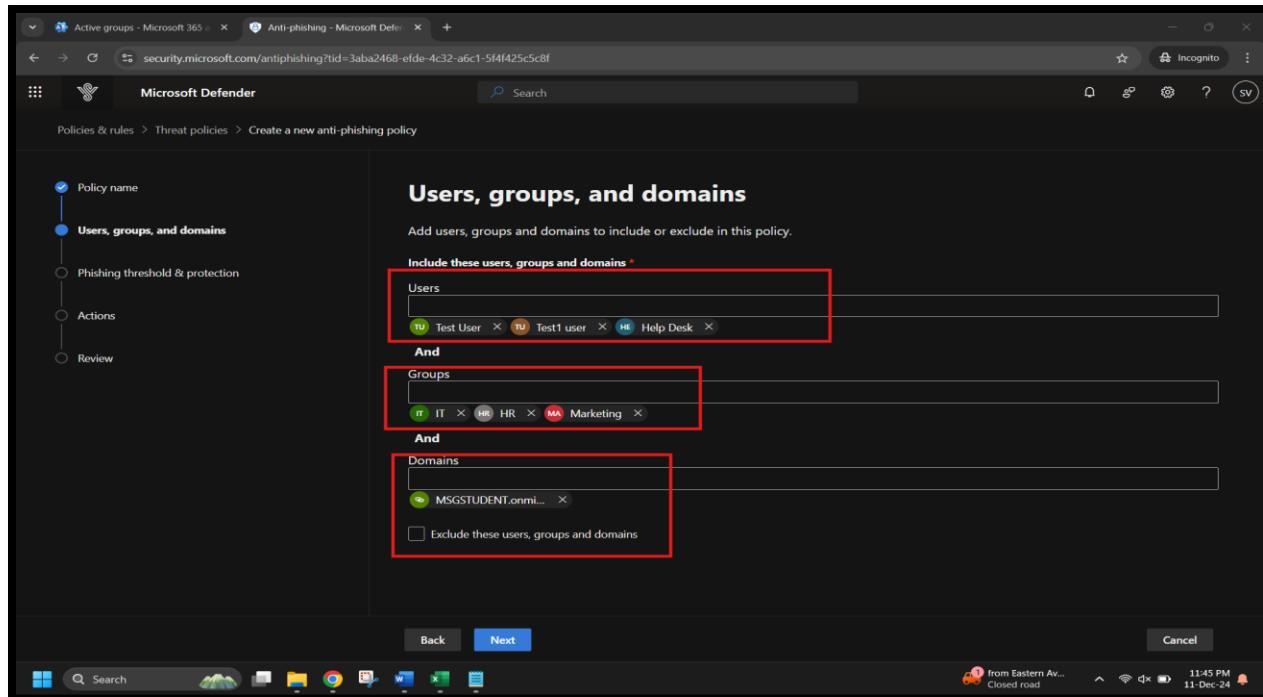
The screenshot shows the Microsoft Defender Threat policies interface, similar to the previous one but with a different focus. The left sidebar is identical. The main content area is titled "Safe attachments" and displays a table of threat policies. A single row is visible, labeled "Built-in protection (Microsoft)" with a status of "On" and priority "Lowest". The entire table row is highlighted with a red box. In the top right corner, there is a user profile for "MSGSTUDENT" and "Shivani Varu".

## Microsoft 365 Identity and Services – Enterprise Administration

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



The screenshot shows the 'Policy name' configuration step in Microsoft Defender. A red box highlights the breadcrumb path 'Policies & rules > Threat policies > Create a new anti-phishing policy'. Another red box highlights the 'Name' field containing 'Phishing Protection Policy' and the 'Description' field containing 'This is Phishing Protection Policy for TechSolutions Inc.'



The screenshot shows the 'Users, groups, and domains' configuration step. A red box highlights the 'Include these users, groups and domains' section, which lists 'Test User', 'Test1 user', and 'Help Desk'. Another red box highlights the 'Groups' section, which lists 'IT', 'HR', and 'Marketing'. A third red box highlights the 'Domains' section, which lists 'MSGSTUDENT.onmicrosoft.com'. A checkbox for 'Exclude these users, groups and domains' is also shown.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Defender interface for creating a new anti-phishing policy. The left sidebar has a checklist with five items: Policy name (checked), Users, groups, and domains (checked), Phishing threshold & protection (checked), Actions (checked), and Review (unchecked). The main area is titled 'Review' and contains the following information:

- Policy name:** Phishing Protection Policy  
[Edit policy name](#)
- Description:** This is Phishing Protection Policy for TechSolutions Inc.  
[Edit policy description](#)
- Users, groups, and domains**
  - Included users:  
testuser@MSGSTUDENT.onmicrosoft.com  
101481565@MSGSTUDENT.onmicrosoft.com  
helpdesk@MSGSTUDENT.onmicrosoft.com
  - Included groups:  
itteam@MSGSTUDENT.onmicrosoft.com  
hrtteam@MSGSTUDENT.onmicrosoft.com  
marketingteam@MSGSTUDENT.onmicrosoft.com
  - Included recipient domains:  
MSGSTUDENT.onmicrosoft.com

At the bottom are 'Back', 'Submit' (highlighted in blue), and 'Cancel' buttons.

The screenshot shows the Microsoft Defender interface for creating a new anti-phishing policy. The left sidebar has a checklist with five items: Policy name (checked), Users, groups, and domains (checked), Phishing threshold & protection (checked), Actions (checked), and Review (unchecked). The main area is titled 'Phishing threshold and protections' and contains the following settings:

- Phishing threshold:** 4 - Most Aggressive
- User impersonation protection:**
  - On for 3 user(s)
- Domain impersonation protection:**
  - On for owned domains
  - Off - 0 domain(s) specified
- Trusted impersonated senders and domains:**
  - Off
- Mailbox intelligence:**
  - On
- Mailbox intelligence for impersonations:**
  - Off (Mailbox intelligence must be turned on to access this)
- Spoof intelligence:**
  - On

Below these settings are 'Edit protection settings' and 'Actions' sections. The 'Actions' section includes:

- If a message is detected as user impersonation: Quarantine the message
- If a message is detected as domain impersonation: Quarantine the message

At the bottom are 'Back', 'Submit' (highlighted in blue), and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Defender Threat Policy creation interface. The left sidebar lists steps: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The main area is titled 'Actions' and contains the following options:

- If a message is detected as user impersonation:
  - Quarantine the message
- If a message is detected as domain impersonation:
  - Quarantine the message
  - DefaultFullAccessPolicy
- If Mailbox Intelligence detects an impersonated user:
  - Don't apply any action
- If the message is detected as spoof and DMARC Policy is set as p=quarantine:
  - Quarantine the message
  - Default full access policy
- If the message is detected as spoof and DMARC Policy is set as p=reject:
  - Reject the message
- If the message is detected as spoof by spoof intelligence:
  - Move the message to the recipients' Junk Email folders
- First contact safety tip
  - On
- User impersonation safety tip
  - On
- Domain impersonation safety tip
  - On
- Unusual characters safety tip
  - On

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

This screenshot shows the same Microsoft Defender Threat Policy creation interface as the first one, but with more detailed actions listed under the 'Actions' section:

- If the message is detected as spoof and DMARC Policy is set as p=quarantine:
  - Quarantine the message
  - Default full access policy
- If the message is detected as spoof and DMARC Policy is set as p=reject:
  - Reject the message
- If the message is detected as spoof by spoof intelligence:
  - Move the message to the recipients' Junk Email folders
- First contact safety tip
  - On
- User impersonation safety tip
  - On
- Domain impersonation safety tip
  - On
- Unusual characters safety tip
  - On
- Unauthenticated senders symbol (?) for spoof
  - On
- Show "via" tag
  - On
- Honor DMARC record policy when the message is detected as spoof
  - On

An 'Edit actions' button is visible at the bottom left of the actions list. At the very bottom are Back, Submit, and Cancel buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows a Microsoft Defender interface for creating a new anti-phishing policy. On the left, a vertical checklist indicates steps completed: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. A large red box highlights the central message: "New anti-phishing policy created" with a green checkmark icon. Below it, a sub-message states: "Your anti-phishing policy **Phishing Protection Policy** has been created. It will go into effect immediately". Under "Related features", there are three links: "View this policy", "View anti-phishing policies", and "Learn more about anti-phishing policies". At the bottom right is a "Done" button.

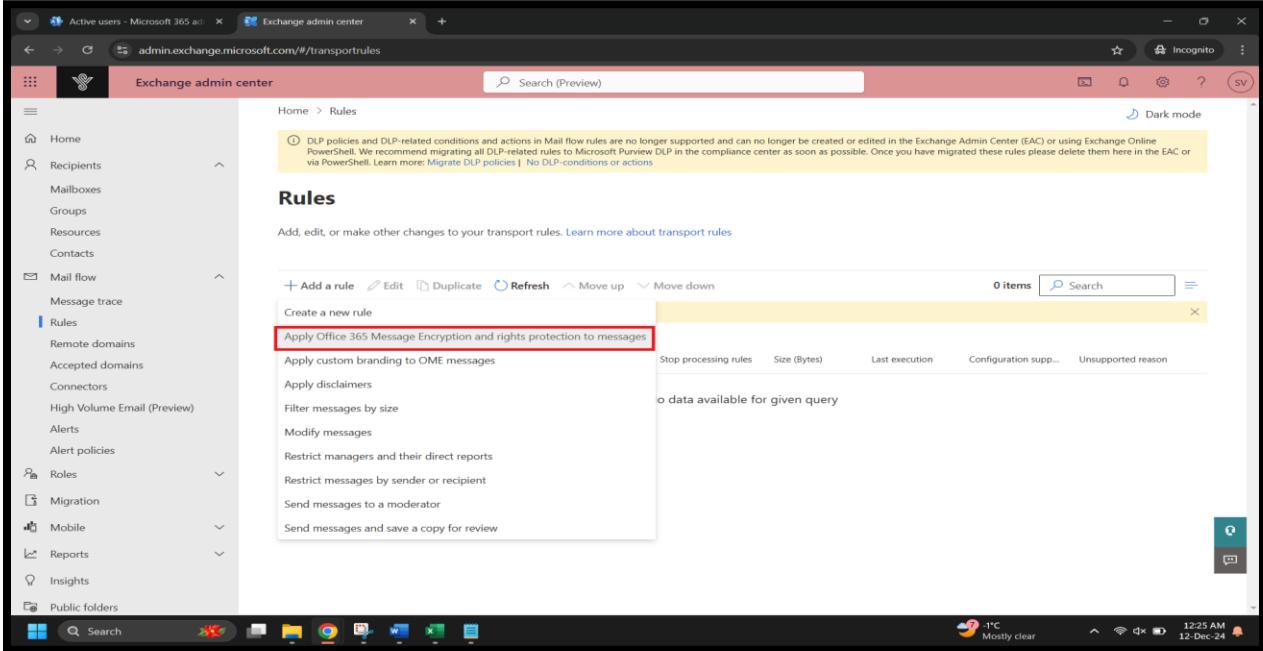
The screenshot shows the Microsoft Defender interface for threat policies. The left sidebar lists categories like Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log, and Policies. A red box highlights the "Anti-phishing" section under "Policies & rules". The main area displays a table of threat policies:

| Name                                  | Status    | Priority | Last modified |
|---------------------------------------|-----------|----------|---------------|
| Phishing Protection Policy            | On        | 0        | Dec 12, 2024  |
| Office365 AntiPhish Default (Default) | Always on | Lowest   | Dec 7, 2024   |

## Microsoft 365 Identity and Services – Enterprise Administration

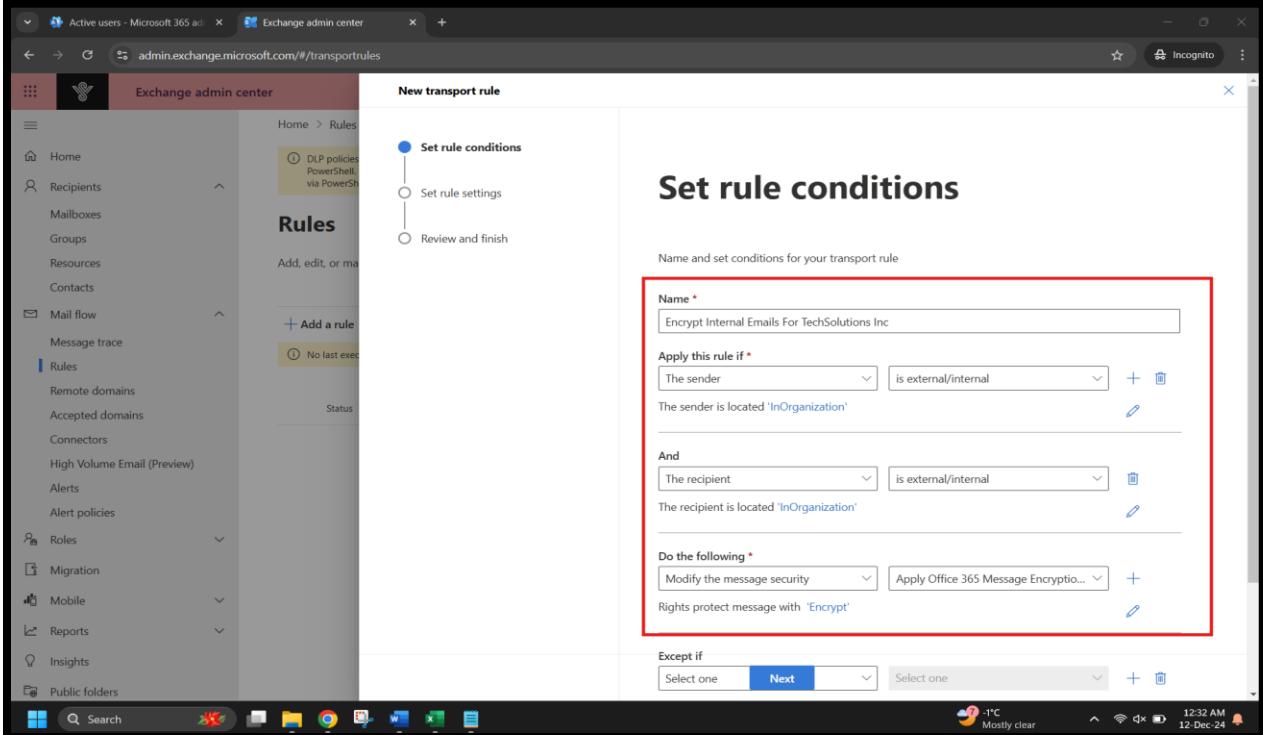
### 2.2 Set Up Data Encryption:

#### Configure Microsoft 365 Message Encryption.



The screenshot shows the Exchange admin center interface. The left sidebar is collapsed. The main area displays the 'Rules' section with a message about DLP policies being deprecated. Below this, there's a list of actions: 'Create a new rule', '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 red box highlights the first option, 'Apply Office 365 Message Encryption and rights protection to messages'.

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



The screenshot shows the 'New transport rule' wizard. The left sidebar is collapsed. The main area shows the 'Set rule conditions' step. It includes fields for 'Name' (set to 'Encrypt Internal Emails For TechSolutions Inc'), 'Apply this rule if' (set to 'The sender is external/internal' and 'The sender is located 'InOrganization''), 'And' (set to 'The recipient is external/internal' and 'The recipient is located 'InOrganization''), 'Do the following' (set to 'Modify the message security' and 'Apply Office 365 Message Encryption...'), and 'Rights protect message with 'Encrypt''. A red box highlights the 'Name', 'Apply this rule if', 'And', 'Do the following', and 'Rights protect message with' sections.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Exchange admin center interface. On the left, the navigation menu includes Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow (selected), Rules (selected), Remote domains, Accepted domains, Connectors, High Volume Email (Preview), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, and Public folders. In the center, the 'Rules' section is selected, showing a 'New transport rule' wizard. The first step, 'Set rule settings', is active. The configuration pane shows:

- Rule mode:** Enforce (radio button selected)
- Severity:** High
- Activate this rule on:** 12/12/2024 - 12:30 AM
- Deactivate this rule on:** 12/12/2024 - 12:30 PM
- Match sender address in message:** Header or envelope

At the bottom, there are 'Comments' and 'Back' and 'Next' buttons.

The screenshot shows the Exchange admin center interface. The navigation menu is identical to the previous screen. In the center, the 'Rules' section is selected, showing the 'New transport rule' wizard at the 'Review and finish' step. The configuration pane displays the rule details:

**Rule name:** Encrypt Internal Emails For TechSolutions Inc  
**Rule comments:** (empty)

| Rule conditions                                                                                            | Rule settings                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apply this rule if:<br>The sender is located 'InOrganization'<br>The recipient is located 'InOrganization' | Mode: Enforce<br>Set date range: - 12/12/2024 12:30 PM<br>Priority: 0<br>Severity: High<br>For rule processing errors: Ignore<br>Stop processing more rules: false<br>Edit rule settings |
| Do the following:<br>Rights protect message with 'Encrypt'                                                 |                                                                                                                                                                                          |
| Except if:<br>Edit rule conditions                                                                         |                                                                                                                                                                                          |

At the bottom, there are 'Back' and 'Finish' buttons.

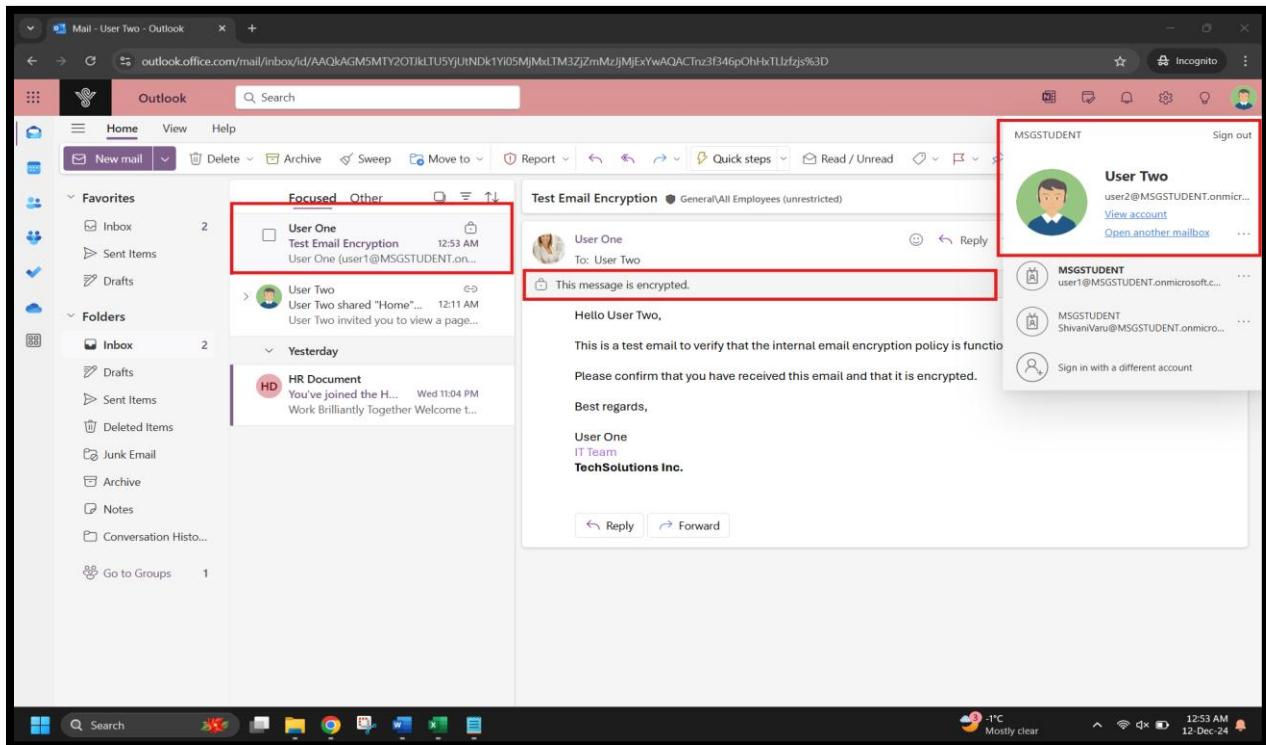
## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Exchange admin center interface. On the left, the navigation menu includes Home, Recipients, Mailboxes, Groups, Resources, Contacts, Mail flow (selected), Message trace, Rules, Remote domains, Accepted domains, Connectors, High Volume Email (Preview), Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, and Public folders. The main content area is titled "Rules" and displays a table of rules. One rule is selected, showing its details: "Rule name: Encrypt Internal Emails For TechSolutions Inc", "Mode: Enforce", "Severity: High", "Senders address: Matching HeaderOrEnvelope", "Priority: 0", and "Status: Enabled". The status bar at the bottom indicates "Rule status updated successfully". The status bar also shows "Cold weather Now", "12:39 AM 12-Dec-24", and a battery icon.

The screenshot shows an Outlook inbox. The left sidebar lists Favorites (Inbox, Sent Items, Drafts) and Folders (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Archive, Notes, Conversation History). A new message is being composed, with the "To" field containing "User Two". The message body starts with "Hello User Two," followed by "This is a test email to verify that the internal email encryption policy is functioning correctly. Please confirm that you have received this email and that it is encrypted." At the bottom of the message, there is a signature for "User One" from "TechSolutions Inc.". The status bar at the bottom indicates "Test Email Encryption", "12:52 AM 12-Dec-24", and a battery icon.

## Microsoft 365 Identity and Services – Enterprise Administration

[ Screenshot: Now, it's confirmed that emails from inside the organization are automatically encrypted]



## Microsoft 365 Identity and Services – Enterprise Administration

### Task 3: Configuring and Managing Collaboration Tools

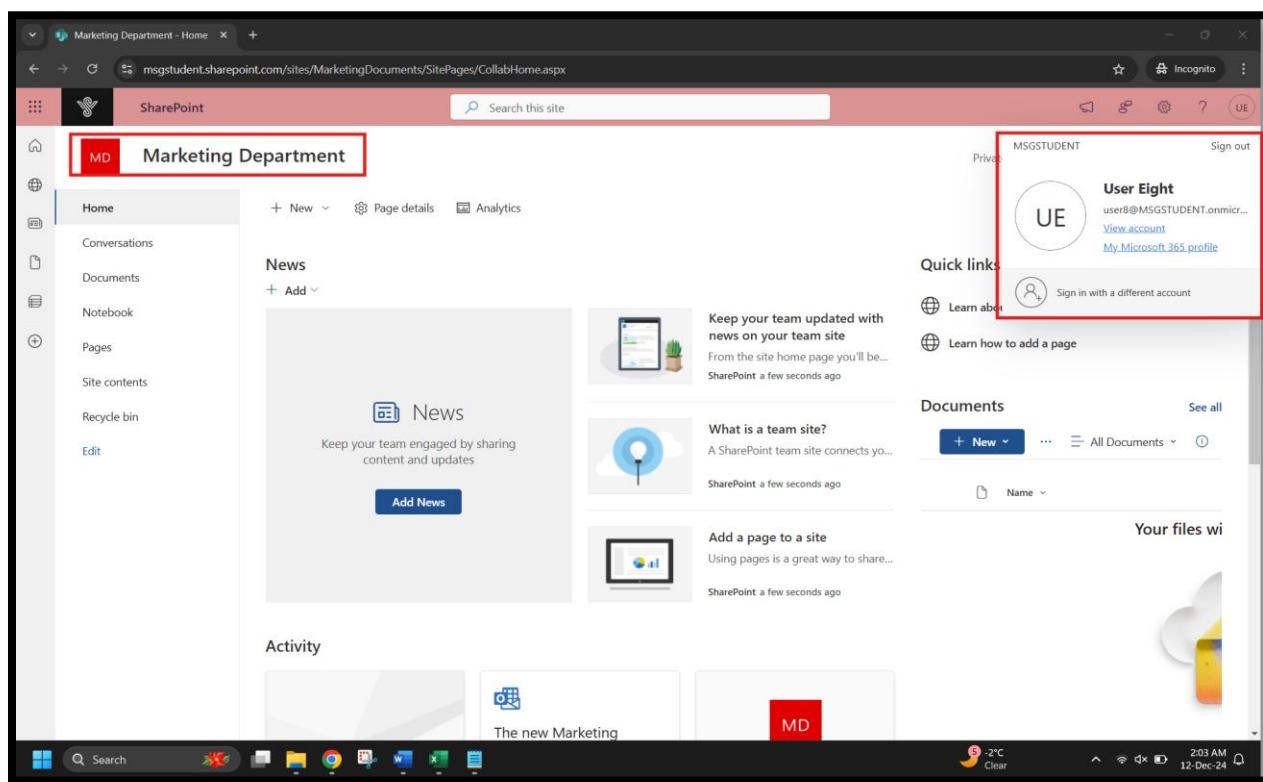
#### 1. Set Up SharePoint Online:

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

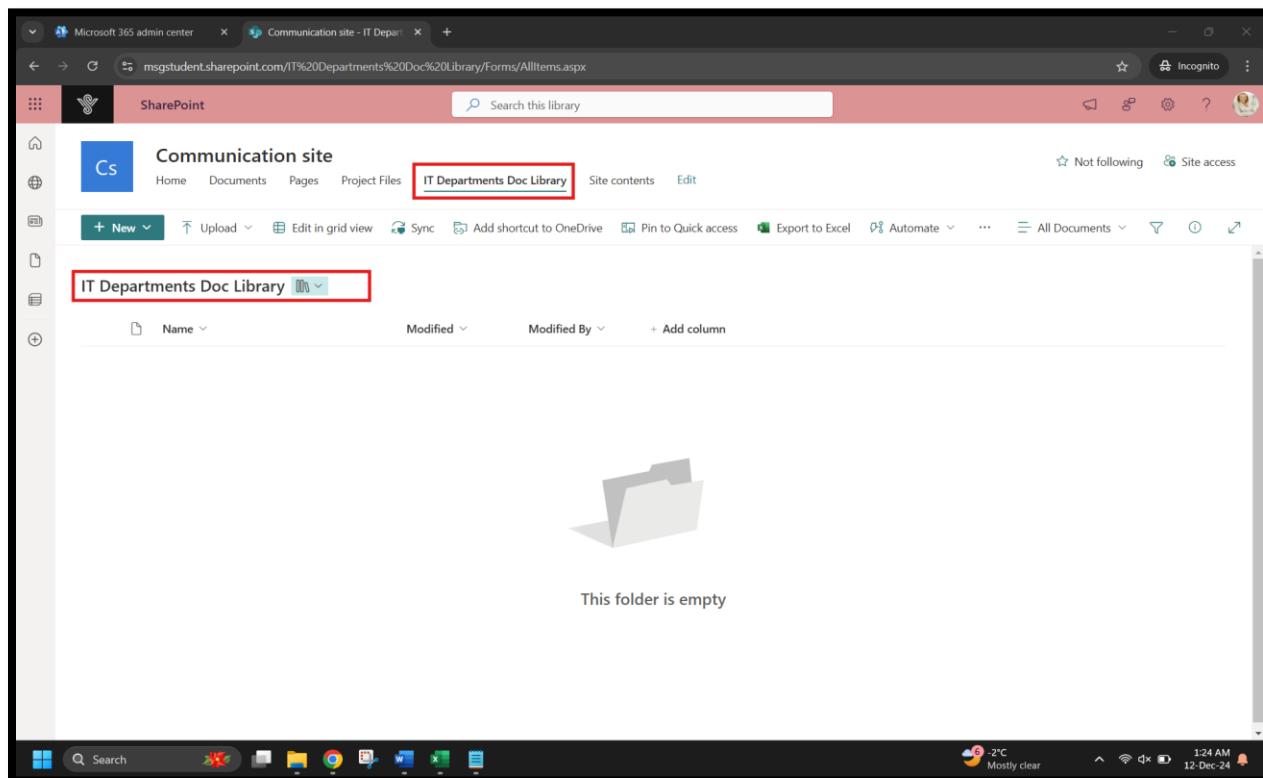
The screenshot shows the SharePoint Online interface for the 'IT Department - Home' site. The top navigation bar includes the SharePoint logo, a search bar, and user information for 'MSGSTUDENT' and 'Shivani Varu'. A red box highlights the site title 'IT Department' in the top left. The left sidebar lists navigation options like Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area features a 'News' section with a 'News' card (Keep your team updated with news on your team site) and a 'What is a team site?' card (A SharePoint team site connects yo...). Below these are 'Documents' and 'Activity' sections. The bottom status bar shows system icons and the date '12-Dec-24'.

The screenshot shows the SharePoint Online interface for the 'HR Department - Home' site. The top navigation bar includes the Microsoft 365 logo, a search bar, and user information for 'MSGSTUDENT' and 'User Two'. A red box highlights the site title 'HR Department' in the top left. The left sidebar lists navigation options like Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area features a 'News' section with a 'News' card (Keep your team updated with news on your team site) and a 'What is a team site?' card (A SharePoint team site connects yo...). Below these are 'Documents' and 'Activity' sections. The bottom status bar shows system icons and the date '12-Dec-24'.

## Microsoft 365 Identity and Services – Enterprise Administration



- Configure document libraries and permissions for each site.



## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the SharePoint Permissions page for the 'IT Dept Library'. The left navigation bar includes links like Home, Conversations, Documents, Notebook, Pages, IT Dept Library, Site contents, and Recycle Bin. The main content area displays a table of permissions:

| Name                  | Type             | Permission Levels |
|-----------------------|------------------|-------------------|
| IT Department Members | SharePoint Group | Edit              |
| IT Department Owners  | SharePoint Group | Full Control      |

A yellow banner at the top states: "This library has unique permissions." A red box highlights the permission table.

This screenshot shows the SharePoint People and Groups page for the 'IT Department Members' group. The left navigation bar is similar to the previous screen. The main content area shows a 'Share 'IT Department'' dialog box:

Share 'IT Department'

Invite people: User One, User Three, User Five, User Seven  
Shared with: Shivani Varu

Please check this site.

SHOW OPTIONS Share Cancel

## Microsoft 365 Identity and Services – Enterprise Administration

[Screenshot: User two (belongs to HR dept) is not allowed, Only IT Dept member can access Document library ]

This screenshot shows the Microsoft 365 SharePoint permissions interface. The left navigation bar includes Home, Conversations, Documents, Notebook, Pages, IT Dept Library, Site contents, and Recycle Bin. The main area displays a 'Check Permissions' dialog for the 'IT Dept Library'. The dialog title is 'IT Dept Library: Check Permissions'. It contains a 'User/Group:' input field with 'User Two' typed in, which is highlighted with a red box. Below the input field are 'Check Now' and 'Close' buttons. A note at the bottom states: 'The user will not be able to browse to the list. The user may need to be granted access to the containing site.' and 'Permission levels given to User Two (i0RfjmembershipUser2@msgstudent.onmicrosoft.com)'. The status 'None' is shown. The taskbar at the bottom shows various application icons and the date/time as 12-Dec-24.

This screenshot shows the Microsoft 365 SharePoint library interface for the 'Marketing Department' site. The left navigation bar includes Home, Conversations, Documents, Shared with us, Notebook, Pages, and a 'Marketing Department ...' item, which is highlighted with a red box. The main area shows a 'Marketing Department Doc Library' with a list view. The table has columns for Name, Modified, and Modified By. A message at the bottom right says 'This folder is empty'. The taskbar at the bottom shows various application icons and the date/time as 12-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the SharePoint 'Permissions' page for the 'Marketing Department' site. The 'PERMISSIONS' tab is selected. A red box highlights the 'Manage Inheritance' button under the 'Inheritance' section. A yellow callout box states: 'There are limited access users on this site. Users may have limited access if an item or document under the site has been shared with them. Show users.' Below this, it says 'This library inherits permissions from its parent. (Marketing Department)'. On the right, a table lists permissions for three groups:

| Name                          | Type             | Permission Levels |
|-------------------------------|------------------|-------------------|
| Marketing Department Members  | SharePoint Group | Edit              |
| Marketing Department Owners   | SharePoint Group | Full Control      |
| Marketing Department Visitors | SharePoint Group | Read              |

The screenshot shows the SharePoint 'People and Groups' page for the 'Marketing Department Members' group. A red box highlights the 'EDIT LINKS' button. A modal dialog box titled 'Share 'Marketing Department'' is open, showing the 'Invite people' section with three users selected: 'User\_Eight', 'User\_Nine', and 'User\_Ten'. The message field contains 'Please check this site.' At the bottom are 'SHOW OPTIONS', 'Share', and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the SharePoint Permissions page for the 'Marketing Department Doc Library'. The left navigation bar includes Home, Conversations, Documents, Notebook, Pages, Marketing Department Doc Library, Site contents, and Recycle Bin. The main content area displays a warning message: 'This library has unique permissions.' Below this, a modal window titled 'Marketing Department Doc Library: Check Permissions' is open, showing the 'Check Permissions' section. It prompts the user to enter a User/Group name, with 'User One' entered. A note below states: 'The user will not be able to browse to the list. The user may need to be granted access to the containing site.' and 'Permission levels given to User One (i0R#membershipuser1@msgstudent.onmicrosoft.com)'. The permission level listed is 'None'. The status bar at the bottom shows the date as 12-Dec-24.

The screenshot shows the SharePoint Home page for the 'HR Department'. The left navigation bar includes Home, Conversations, Documents, Shared with us, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area features a large 'HR Department' header with a red border. Below it is a 'HR Department Doc Library' section with a red border around its title. The page displays a grid view of the library with columns for Name, Modified, and Modified By. A message at the bottom right says 'This folder is empty'. The status bar at the bottom shows the date as 12-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the SharePoint Permissions page for the 'HR Department Doc Library'. The 'PERMISSIONS' tab is selected. A red box highlights the 'Stop inheriting Permissions' button under the inheritance section. The main content area displays a table of users and their permission levels:

| Name                   | Type             | Permission Levels |
|------------------------|------------------|-------------------|
| HR Department Members  | SharePoint Group | Edit              |
| HR Department Owners   | SharePoint Group | Full Control      |
| HR Department Visitors | SharePoint Group | Read              |

Below the table, there are two yellow warning boxes: one about limited access users and another about people waiting for approval.

[Screenshot: I assigned the appropriate permissions to the HR Confidential group by selecting 'Contribute' to allow file editing and restricting unauthorized access ]

This screenshot shows the SharePoint 'Share' dialog for the 'HR Department Doc Library'. The 'Grant Permissions' button is highlighted with a red box. The dialog content includes:

- A header: 'Share 'HR Department Doc Library' and its contents'
- A 'Shared with lots of people' section showing 'User Six' and 'User Four' with a red box.
- A message: 'You have been granted access to the HR Documents library for managing sensitive HR data.'
- An unchecked checkbox: 'Share everything in this folder, even items with unique permissions.'
- A 'HIDE OPTIONS' section with:
  - A checked checkbox: 'Send an email invitation'
  - A dropdown menu: 'Select a permission level' set to 'Contribute' (highlighted with a red box).
- Buttons at the bottom: 'Share' and 'Cancel'.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the Microsoft SharePoint 'Permissions' interface for the 'HR Department Doc Library'. The 'Check' tab is selected. A modal window titled 'HR Department Doc Library: Check Permissions' is open, showing the permission levels for 'User Two'. The modal includes fields for 'User/Group' (set to 'User.Two') and buttons for 'Check Now' and 'Close'. Below the modal, a detailed list of permissions is provided:

| Permission Level | Description                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Control     | Given through the "HR Department Owners" group.                                                                                                          |
| Edit             | Given through the "HR Department Members" group.                                                                                                         |
| Deny             | Add and Customize: Add, change, or delete HTML pages or Web Part Pages, and edit the Web site using a Microsoft SharePoint Foundation-compatible editor. |

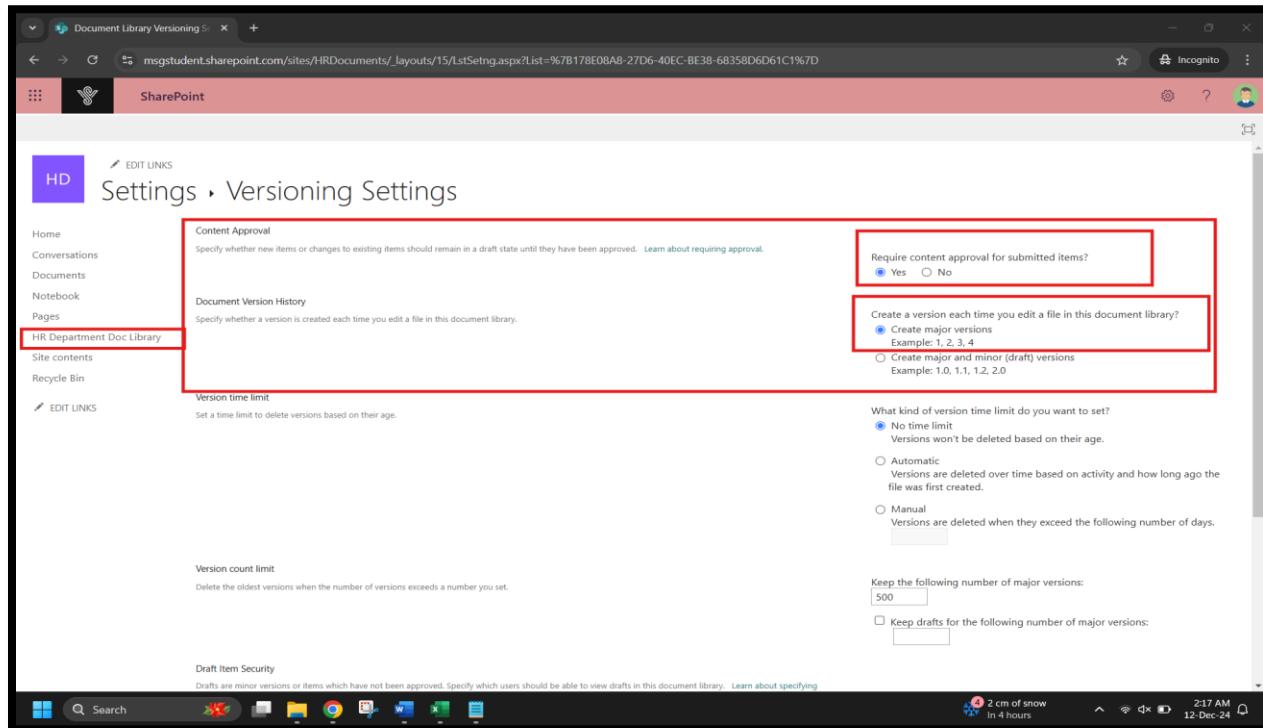
The SharePoint ribbon at the top has 'PERMISSIONS' selected. The left navigation pane shows 'Documents' and 'Pages' under 'HR Department Doc Library'. The taskbar at the bottom shows various pinned icons and the date '12-Dec-24'.

This screenshot shows the Microsoft SharePoint 'Permissions' interface for the 'HR Department Doc Library'. The 'Check' tab is selected. A modal window titled 'HR Department Doc Library: Check Permissions' is open, showing the permission levels for 'User Three'. The modal includes fields for 'User/Group' (set to 'User.Three') and buttons for 'Check Now' and 'Close'. Below the modal, a message states: 'The user will not be able to browse to the list. The user may need to be granted access to the containing site.' A note also mentions: 'Permission levels given to User Three (i0RJfmembership\user3@msgstudent.onmicrosoft.com) None'.

The SharePoint ribbon at the top has 'PERMISSIONS' selected. The left navigation pane shows 'Documents' and 'Pages' under 'HR Department Doc Library'. The taskbar at the bottom shows various pinned icons, a weather forecast for 'Snow coming In about 2 hours', and the date '12-Dec-24'.

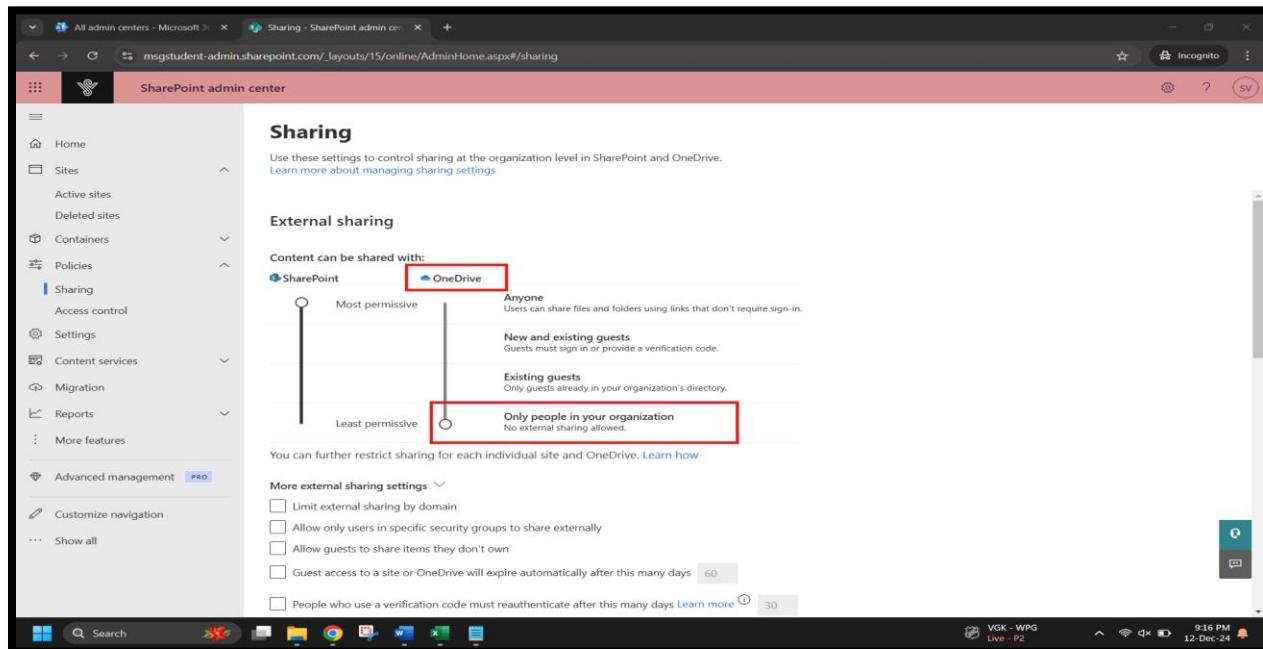
## Microsoft 365 Identity and Services – Enterprise Administration

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



### 3.2 Implement OneDrive for Business:

- Configure OneDrive settings to restrict external sharing.



## Microsoft 365 Identity and Services – Enterprise Administration

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more about managing sharing settings](#).

**File and folder links**

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

Specific people (only the people the user specifies)

Only people in your organization

Anyone with the link

Choose the permission that's selected by default for sharing links.

View

Edit

Choose expiration and permissions options for Anyone links.

These links must expire within this many days

These links can give these permissions:

Files:

Folders:

**Other settings**

OneDrive

IT Document

msgstudent.sharepoint.com/w/r/sites/ITDocuments/\_layouts/15/Doc.aspx?... Live - P2 9:17 PM 12-Dec-24

File Home Insert Layout References Review View Help

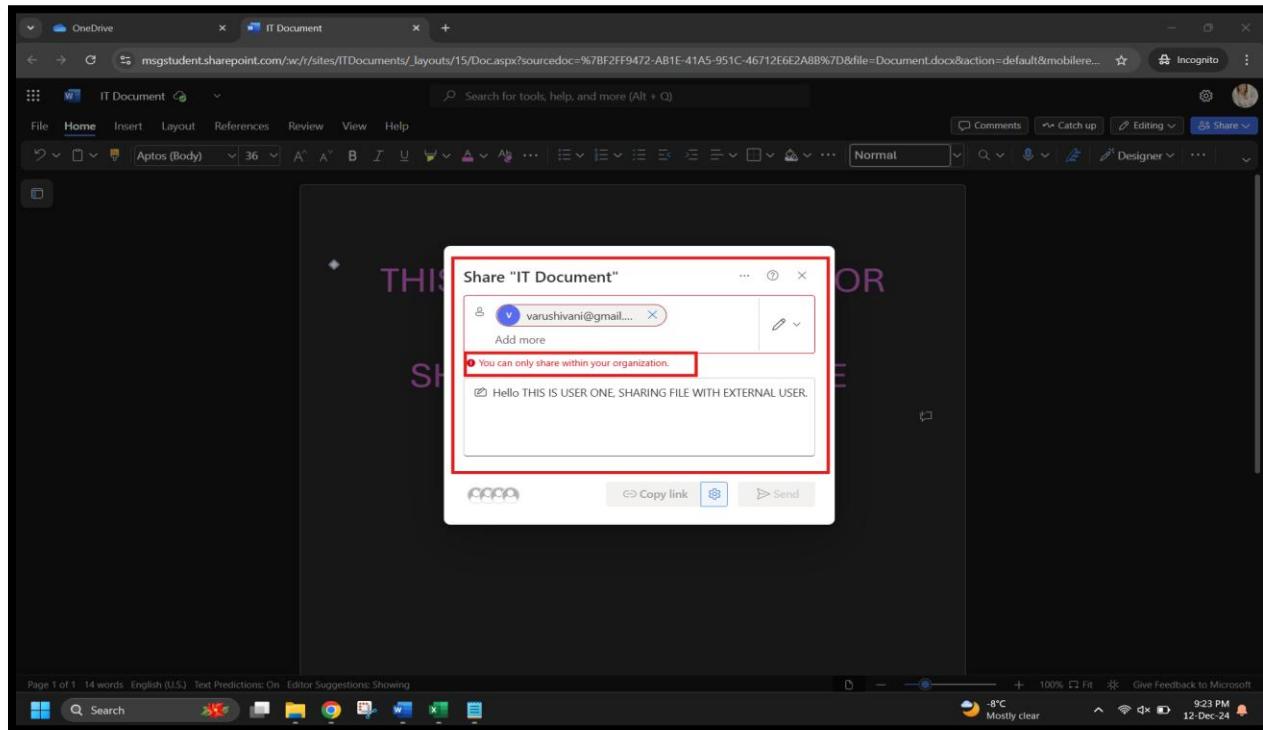
Comm MSGSTUDENT Sign out

User One  
user1@MSGSTUDENT.onmicrosoft.com  
View account  
My Microsoft 365 profile

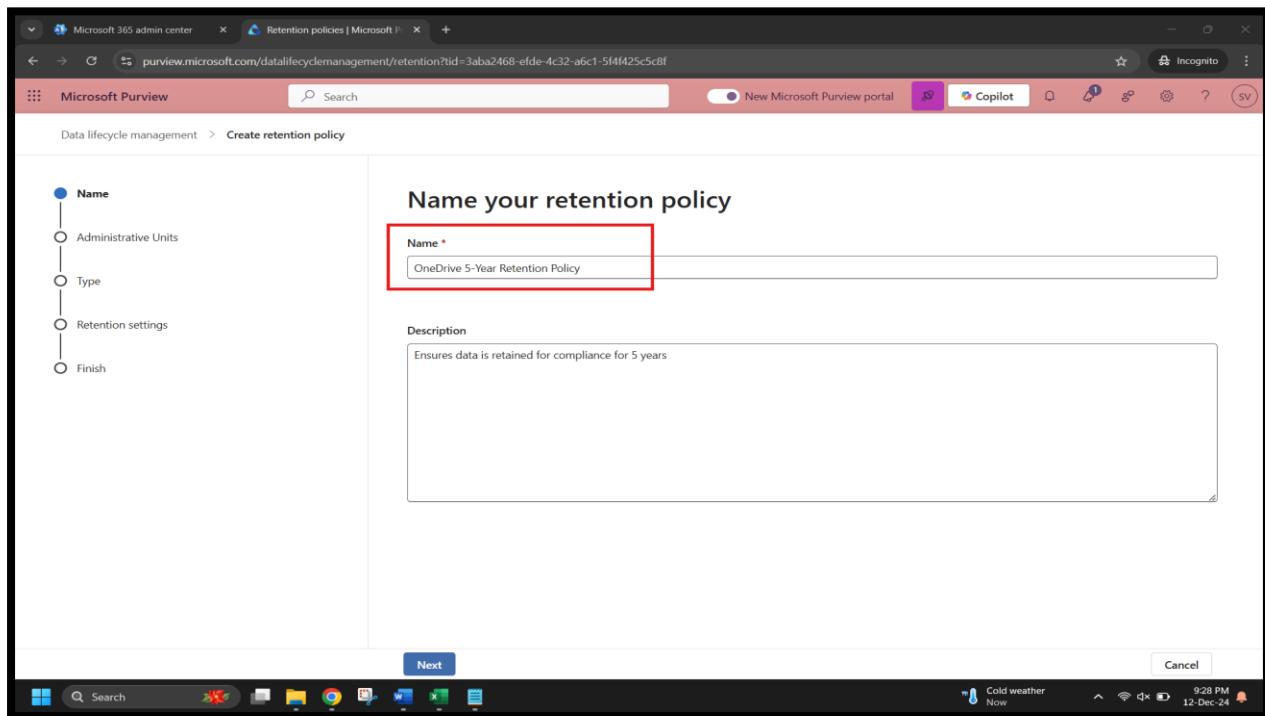
THIS IS TEST DOCUMENT FOR  
CHECKING EXTERNAL  
SHARING from USER ONE  
[ IT MANAGER]

## Microsoft 365 Identity and Services – Enterprise Administration

[Screenshot: user one trying to share document with external user, but it cannot share ]



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



## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Choose where to apply this policy' step of the retention policy creation wizard. On the left, a sidebar lists steps: Name, Administrative Units, Type (selected), Locations, Retention settings, and Finish. The main area displays a table of locations with their status, location, applicable content, included users, and excluded users. One row for 'OneDrive accounts' has its 'On' toggle switch highlighted with a red box.

| Status    | Location                                   | Applicable Content                                                                                                                                                                                                                                                                      | Included                 | Excluded    |
|-----------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------|
| 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. <a href="#">More details</a>                                                                        | All user accounts        | Edit        |
| 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). <a href="#">More details</a>                                                                 |                          |             |
| <b>On</b> | <b>OneDrive accounts</b>                   | <b>All files in users' OneDrive accounts. <a href="#">More details</a></b>                                                                                                                                                                                                              | <b>All user accounts</b> | <b>None</b> |
| 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. <a href="#">More details</a> |                          |             |
| Off       | Skype for Business                         | Skype conversations for the users you choose.                                                                                                                                                                                                                                           |                          |             |

The screenshot shows the 'Decide if you want to retain content, delete it, or both' step of the wizard. The sidebar now includes 'Retention settings' (selected). The main area contains three radio button options: 'Retain items for a specific period' (selected), 'Retain items forever', and 'Only delete items when they reach a certain age'. The 'Retain items for a specific period' section is highlighted with a red box, showing a dropdown for '5 years' and a dropdown for 'Start the retention period based on' set to 'When items were created'. Below these are two additional options: 'When items were last modified' and 'Do nothing'.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Create retention policy' review and finish step. On the left, a vertical checklist indicates steps completed: Name (checkmark), Administrative Units (checkmark), Type (checkmark), Retention settings (checkmark), and Finish (blue dot). The main area displays the policy details:

- Review and finish**: A summary message states it will take up to a week to apply the policy to selected locations.
- Policy name**: OneDrive 5-Year Retention Policy (with [Edit](#) link).
- Description**: Ensures data is retained for compliance for 5 years (with [Edit](#) link).
- Locations to apply the policy**: OneDrive accounts (All Sites) (with [Edit](#) link).
- Retention settings**: Retain items for 5 years based on when they were created; Delete items at end of retention period (with [Edit](#) link).

A warning message at the bottom notes: "⚠ 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 [Back](#), [Submit](#), and [Cancel](#) buttons. The taskbar at the bottom shows various application icons and the date/time: Sunday, 12-Dec-24.

The screenshot shows the 'Create retention label' review and finish step. On the left, a vertical checklist indicates steps completed: Name (checkmark), Label Settings (checkmark), Period (checkmark), and Finish (blue dot). The main area displays the label details:

- Review and finish**: A summary message states it will take up to a week to apply the label to selected users.
- Name**: Test Retention Policy (with [Edit](#) link).
- Description for users**: Test Retention Policy for One Drive for 5 years (with [Edit](#) link).
- Description for admins**: Test Retention Policy for One Drive for 5 years (with [Edit](#) link).
- Retention settings**:
  - Retention period**: 5 years (with [Edit](#) link).
  - Retention action**: Retain and Delete (with [Edit](#) link).
  - Based on**: Based on when it was created (with [Edit](#) link).

At the bottom are [Back](#), [Create label](#), and [Cancel](#) buttons. The taskbar at the bottom shows various application icons and the date/time: Sunday, 12-Dec-24.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Data Lifecycle Management Labels page. On the left, there's a navigation sidebar with 'Data Lifecycle Management' selected. Under 'Retention labels', it shows 'Policies' with 'Retention policies' expanded, showing 'Test Retention Policy'. The main area is titled 'Labels' and contains a brief description of what labels are used for. It lists 'Test Retention Policy' and provides details about its retention duration (5 years), type (Auto-delete), and creation information (created by Shivani Varu on Dec 12, 2024). The status bar at the bottom indicates it's 9:45 PM on Dec 12.

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

The screenshot shows the 'Create retention policy' wizard on the 'Name your retention policy' step. On the left, a vertical navigation bar lists steps: Name, Administrative Units, Type, Retention settings, and Finish. The 'Name' step is currently active. The main area has a red border around the 'Name' field, which contains 'OneDrive Old Files Deletion After 1 Year'. Below it is a 'Description' field with the text 'The purpose for this retention policy is for OneDrive Old Files Deletion After 1 Year to recycle bin'. At the bottom right are 'Next' and 'Cancel' buttons. The status bar at the bottom indicates it's 9:53 PM on Dec 12.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Data lifecycle management 'Create retention policy' wizard. The current step is 'Choose the type of retention policy to create'. A vertical navigation bar on the left lists steps: Name, Administrative Units, Type (which is selected), Retention settings, and Finish. The main content area contains two options: 'Adaptive' and 'Static'. The 'Static' option is selected and highlighted with a red box. A note below it states: 'You'll choose locations containing the content you want to retain. If locations change after this policy is created (for example if a SharePoint site is added or removed), you'll need to manually update the policy.'

The screenshot shows the Microsoft Purview Data lifecycle management 'Create retention policy' wizard. The current step is 'Choose where to apply this policy'. The vertical navigation bar on the left lists steps: Name, Administrative Units, Type (selected), Locations (which is selected), Retention settings, and Finish. The main content area contains a table titled 'Choose where to apply this policy'. It lists five location types with their status and applicable content:

| Status | Location                                   | Applicable Content                                                                                                                                                                                                                                                                      | Included          | Excluded |
|--------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------|
| 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. <a href="#">More details</a>                                                                        | All user accounts | None     |
| 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). <a href="#">More details</a>                                                                 | Edit              | None     |
| On     | OneDrive accounts                          | All files in users' OneDrive accounts. <a href="#">More details</a>                                                                                                                                                                                                                     | All user accounts | None     |
| 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. <a href="#">More details</a> | Edit              | None     |
| Off    | Skype for Business                         | Skype conversations for the users you choose.                                                                                                                                                                                                                                           |                   |          |

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Retention settings' step of the 'Create retention policy' wizard. On the left, a progress bar indicates steps: Name (checkmark), Administrative Units (checkmark), Type (checkmark), Retention settings (selected, blue dot), and Finish. The main area is titled 'Decide if you want to retain content, delete it, or both'. It offers three options:

- Retain items for a specific period: Items will be retained for the period you choose.
- Retain items forever: Items will be retained forever, even if users delete them.
- Only delete items when they reach a certain age: Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

For the 'Only delete items when they reach a certain age' option, there are fields to specify the age: 'Delete items older than' (1 year, 0 months, 0 days) and a dropdown for 'Delete content based on' (set to 'When items were created'). A red box highlights this section.

The screenshot shows the 'Review and finish' step of the 'Create retention policy' wizard. The progress bar shows steps: Name, Administrative Units, Type, Retention settings (selected, blue dot), and Finish. The main area displays the policy details:

- Policy name:** OneDrive Old Files Deletion After 1 Year  
[Edit](#)
- Description:** The purpose for this retention policy is for OneDrive Old Files Deletion After 1 Year to recycle bin  
[Edit](#)
- Locations to apply the policy:** OneDrive accounts (All Sites)  
[Edit](#)
- Retention settings:** Delete items at end of retention period  
Delete items that are older than 1 years based on when they were created  
[Edit](#)

A red box highlights the 'Retention settings' section. A warning message at the bottom states: '⚠️ Items that are currently older than 1 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.'

## Microsoft 365 Identity and Services – Enterprise Administration

### 3.3 Set Up Viva Engage for Enterprise Social Networking:

Configure Viva to allow only internal communications.

Network  
Success  
Configuration  
Design  
Admins  
Usage Policy  
External Networks  
Network Migration  
New Viva Engage

Users  
Remove Users  
Export Users  
Profile Fields

Content and Security  
Monitor Keywords  
Report Conversations  
Security Settings  
Export Network Data  
Export User Data  
Data Retention  
Content Mode

**Security Settings**

**External Messaging**

Viva Engage allows community admins to add people outside your organization to their Viva Engage communities to foster collaboration. Learn More

Allow community admins to add external users to their communities?

Allow

Deny

**Office 365 Identity Enforcement**

Whenever enforcing Office 365 identity, be mindful that this setting replaces any existing Viva Engage SSO setup and ensures that users log in to Viva Engage with their Office 365 accounts. Learn More

Enforce Office 365 identity

Status: Committed

Block Office 365 users without Viva Engage licenses

**Office 365 Connected Viva Engage Groups**

Once your organization has committed to enforcing Office 365 identity and has one Office 365 tenant associated with a single Viva Engage network, connected groups will be enabled for this network. Learn More

Status: Enabled Connected Groups are turned on for this network.

Save

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

Home  
Test User

Explore  
Communities  
Storylines

Favorites  
Keep your favorites at your fingertips. Favorites will appear here. Learn more

Communities  
All Company  
Discover communities

**Create a new community**

Name \*  
Company Wide Announcements for TechSolutions Inc.

Description  
Central hub for company-wide updates, news, and announcements to keep all TechSolutions Inc. employees informed and connected.  
24 characters remaining

Members  
User One User Two User Ten Add people by name or e...

Edit settings

Select public or private community  
Public: anyone in your network can view and join this community.

Communication configurations

Default publisher  
Discussion

Allow all network users to move conversations into this community  
Admins are always able to move conversations

Create

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the Microsoft Viva Engage - Company Wide interface. The main area displays a community feed titled "Company Wide Announcements for TechSolutions Inc". The feed includes sections for Conversations, About, Files, and Events. A large red box highlights the central feed area. On the left, there's a sidebar with options like Home, Test User, Explore, and Favorites. On the right, there are panels for Members (1 member), Info, and Pinned, along with a "Create live event" button.

This screenshot shows the "Create a new community" dialog box overlaid on the Microsoft Viva Engage interface. The dialog has several fields highlighted with red boxes: "Name" (containing "IT Discussions"), "Members" (listing "User One", "User Three", "User Five", and "User Seven"), and "Select public or private community" (set to "Private"). Other visible settings include "Edit settings" and "Communication configurations". The background shows the company-wide feed and navigation sidebar.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the Microsoft Viva Engage interface. On the left, the navigation bar includes Home, Test User, Explore (Communities, Storylines), Favorites, and Communities (All Company, Discover communities). The main area displays the 'IT Discussions' community, which is highlighted with a red border. The community info card shows 1 member, a purple background illustration, and a 'Private' status. Below the card, tabs for Conversations, About, Files, and Events are visible. A large green checkmark icon is centered at the bottom of the page.

This screenshot shows the 'Create a new community' dialog box overlaid on the Viva Engage interface. The dialog has several fields highlighted with red boxes: 'Name' (containing 'HR Announcements'), 'Members' (listing 'User Two', 'User Four', 'User Six', and a placeholder 'Add people by name or email...'), and 'Select public or private community' (set to 'Private: only approved community members can view or participate'). Other visible settings include 'Communication configurations' (Default publisher: Discussion) and a toggle switch for allowing network users to move conversations into the community. The background shows the same 'IT Discussions' community page as the previous screenshot.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Viva Engage interface. On the left, there's a navigation bar with 'Home', 'Test User', 'Explore', 'Communities', 'Storylines', 'Favorites', and 'Communities'. Under 'Communities', it shows 'All Company' and 'Discover communities'. The main area displays a community titled 'HR Announcements' with a purple icon containing 'HA'. A red box highlights this icon. Below the title, it says 'This group is for TechSolutions Inc's HR related announcement'. To the right, there's a 'Members' section (1 member), an 'Info' section, a 'Pinned' section, and a 'Create live event' button. At the bottom, there are tabs for 'Conversations', 'About', 'Files', and 'Events', along with 'Recent posts' and 'All conversations' buttons. A large green checkmark icon is centered at the bottom.

The screenshot shows the Microsoft Viva Engage interface with a 'Create a new community' dialog box open. The 'Name' field is filled with 'Marketing Insights' and is highlighted with a red box. The 'Description' field contains 'This group is for TechSolutions Inc's Marketing team.' Below it, the 'Members' field shows four users: 'User Eight', 'User Nine', 'User Ten', and 'Add people by name or ...', all enclosed in a red box. The 'Edit settings' section has a dropdown menu set to 'Private: only approved community members can view or participate.', which is also highlighted with a red box. The 'Communication configurations' section includes a 'Default publisher' dropdown set to 'Discussion' and a toggle switch for 'Allow all network users to move conversations into this community'. At the bottom right of the dialog is a 'Create' button.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Viva Engage platform. On the left, there's a sidebar with navigation links like Home, Test User, Explore, Communities, Storylines, Favorites, and Communities. The main area features a large banner titled 'MARKETING TEAM' with an illustration of people working at desks. Below the banner is a box for 'Marketing Insights' which says 'This group is for TechSolutions Inc's Marketing team.' It has tabs for Conversations, About, Files, and Events. A red box highlights the 'Conversations' tab. Below this is a section for sharing thoughts, ideas, or updates with buttons for Discussion, Question, Praise, and Poll. At the bottom right of the main area is a green checkmark icon.

Ensure compliance with the company's social media policy.

The screenshot shows the Microsoft Viva Engage Admin Center. On the left, there's a sidebar with Home, Test User, Explore, Communities, Storylines, Favorites, and Communities. The main area is titled 'Custom usage policy' and contains fields for 'Policy name' (set to 'Internal Collaboration Guidelines') and 'Enable policy reminder on Viva Engage home feed' (set to 'On'). Below this is a 'Policy reminder' section with a message about following collaboration guidelines. The 'Policy' section contains a rich text editor with HTML code defining the internal collaboration policy. A red box highlights the policy text area. At the bottom right of the dialog is a 'Save' button.

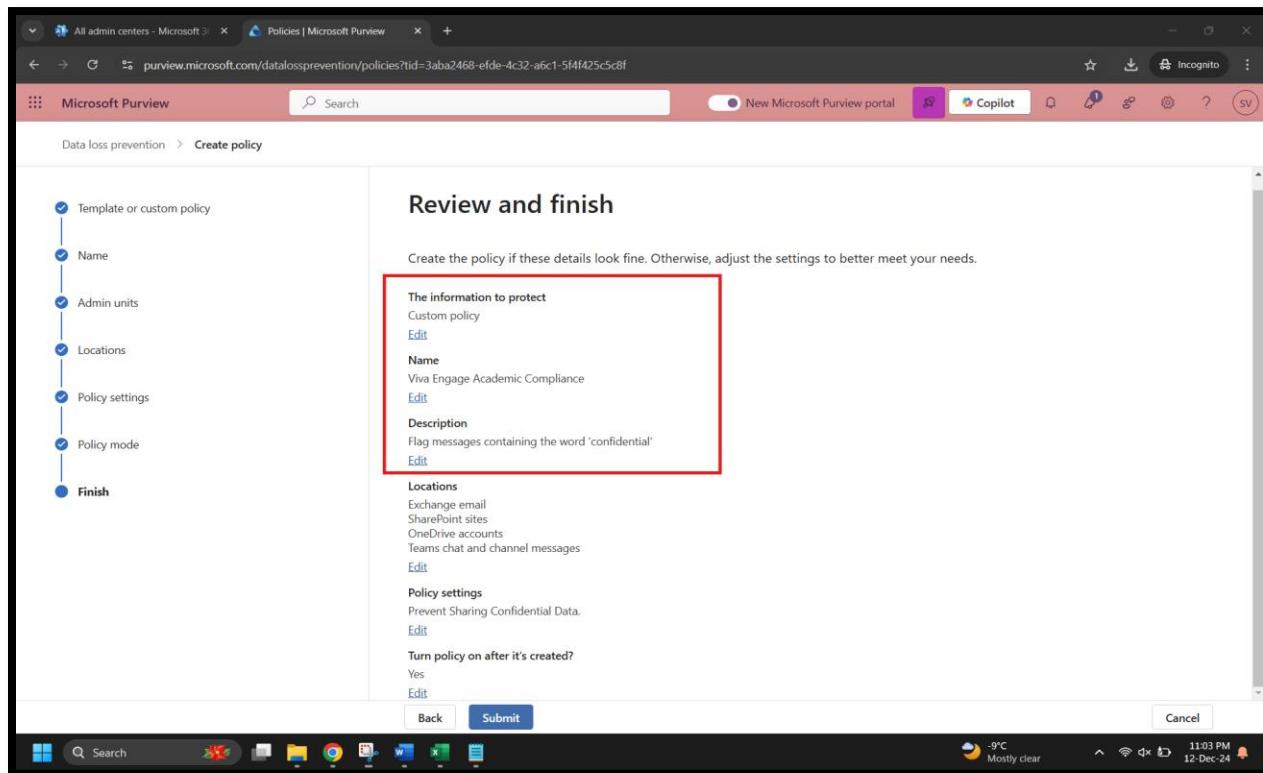
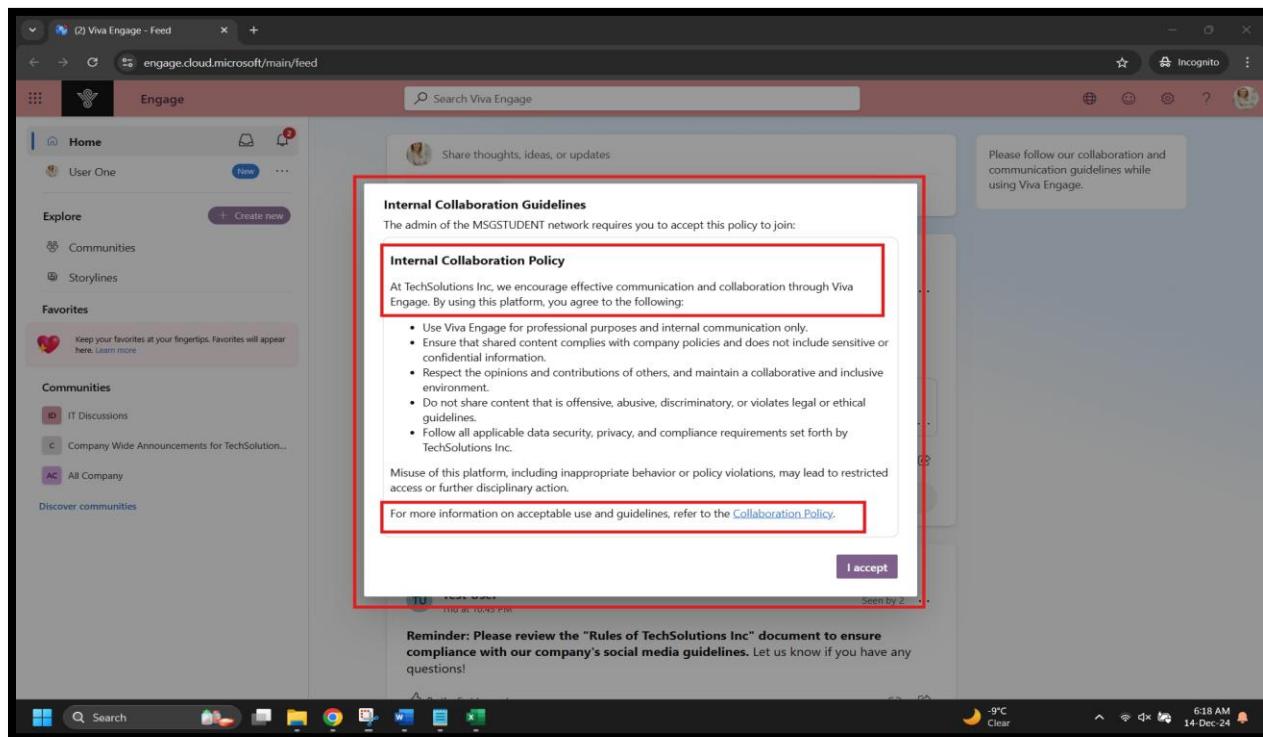
## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Report Conversations' settings page. On the left, there's a sidebar with categories like Network, Success, Configuration, Design, Admins, Usage Policy, External Networks, Network Migration, New Viva Engage, Users, Content and Security, and Report Conversations. The 'Report Conversations' section is highlighted with a red box. It contains a sub-section for 'Report recipient' where an email address is entered: 'ShivaniVaru@MSGSTUDENT.onmicrosoft.com'. Below it is a note: 'In case a report is sent to the above email address, user reporting the conversation will receive a copy of the email'. Another red box highlights the 'Pre-submission details or instructions for user' section, which includes a note about sending reports to the Compliance Team and a link to 'Collaboration Guidelines'. A character count of '1157 characters remaining' is shown at the bottom.

The screenshot shows the 'Post-submission instructions to user (optional)' settings page. The sidebar on the left has sections for Export User Data, Data Retention, and Content Mode. The main area contains a note about reporting to the Compliance Team and a link to 'Collaboration Guidelines'. A red box highlights the 'Post-submission instructions to user (optional)' section, which includes a note about receiving a response from the Compliance Team, a message of thanks, a note about further action, and a link to 'Company Communication Guidelines'. A character count of '887 characters remaining' is shown at the bottom. A 'Save' button is visible at the bottom left.

## Microsoft 365 Identity and Services – Enterprise Administration

[ Screenshot: Sign in as User one , Viva Engage prompts users to accept Internal Collaboration Guidelines outlining usage policies and compliance requirement ]



## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Policies page. On the left, there's a navigation sidebar with options like Home, Communication Compliance (selected), Overview, Policies (selected), Classifiers, Related solutions, Information Barriers, and Insider Risk Management. The main area displays a 'Policies' summary with 0 Policy warnings, 0 Policy recommendations, and 1 Healthy policy. A yellow callout box says 'Some user reported messages contain workplace safety violations. Open the policy to view the policy automatically created by Microsoft to detect Teams and Viva Engage messages that users reported as inappropriate.' Below this is a 'Create Inappropriate Content' button. To the right, a large panel titled 'Monitor communications for inappropriate content' is open. It includes sections for 'About this template', 'Settings we need from you' (with a 'Policy name' field containing 'Social Media Compliance' highlighted with a red box), 'Users or groups in scope' (set to 'All users'), 'Reviewers' (listing 'Test User' and 'Shivani Varu' with a red box around the input field), and 'Settings we've filled in for you'. At the bottom are 'Create policy' and 'Customize policy' buttons.

This screenshot is similar to the one above but shows more detailed configurations for the 'Monitor communications for inappropriate content' template. The 'Communications to detect' section is highlighted with a red box, showing 'Scoped locations' set to 'Teams, Viva Engage'. The 'Conditions and percentage' section is also highlighted with a red box, showing 'Communication direction' as 'Internal', 'Percentage to review' as '100', 'Optical character recognition(OCR)' as 'Disabled', and 'Filter email blasts' as 'Disabled'. The 'Detect content matching these trainable classifiers' section is highlighted with a red box, listing 'Sexual', 'Violence', 'Hate', and 'Self-harm' as trainable classifiers. The rest of the interface is identical to the first screenshot.

## Microsoft 365 Identity and Services – Enterprise Administration

[Screenshot: Social Media Compliance' custom policy setup in Microsoft Purview to monitor and enforce guidelines in Viva Engage ]

**Review and finish**

**Name and description**

**Name**  
Social Media Compliance

**Description**  
This policy monitors and enforces compliance with the company's social media guidelines. It detects inappropriate content in Teams chats, Viva Engage, and email communications, ensuring internal communication standards are met.

**Users and reviewers**

Choose users and groups  
All users

Excluded users and groups  
testuser@msgstudent.onmicrosoft.com, shivanivar@msgstudent.onmicrosoft.com

Reviewers  
testuser@msgstudent.onmicrosoft.com, shivanivar@msgstudent.onmicrosoft.com

**Locations**

Scoped locations  
Viva Engage

**Conditions and percentage**

Communication direction  
Internal

Back Save Cancel

**Communication compliance > Edit Social Media Compliance**

**Name**

**Users and reviewers**

**Locations**

**Conditions and percentage**

Communication direction  
Internal

Optical character recognition(OCR)  
Disabled

Filter email blasts  
Disabled

Conditions  
Content matches contains any of these trainable classifiers: Sexual, Violence, Hate, Self-harm, Unauthorized disclosure, Corporate Sabotage

Percentage to review  
100

Reduce review percentage. Your current percentage might generate a large number of alerts per day.  
Reduce percentage

Back Save Cancel

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Policies page. The left sidebar has a 'Communication Compliance' section selected, indicated by a red box. The main area is titled 'Policies' and displays three categories: Policy warnings (0), Policy recommendations (1), and Healthy policies (0). A table lists one item: 'Social Media Compliance'. The table columns are: Policy name, Messages scanned today, New pending to..., Total pending, Total resolved, Status, and Policy health. The 'Policy name' column shows 'Social Media Compliance'. The 'Policy health' column shows 'Active' with a green checkmark and '1 recommend'.

| Policy name             | Messages scanned today | New pending to... | Total pending | Total resolved | Status | Policy health |
|-------------------------|------------------------|-------------------|---------------|----------------|--------|---------------|
| Social Media Compliance | 0                      | 0                 | 0             | 0              | Active | 1 recommend   |

## Microsoft 365 Identity and Services – Enterprise Administration

### Task 4: Monitoring and Reporting

#### 4.1 Configure Audit Logs:

- Enable and configure audit logging in the Microsoft 365 compliance center.
- Create a custom audit log search to track user activities related to at least one activity in SharePoint such as updating the site content.

The screenshot shows the Microsoft Purview Audit interface. On the left, there's a sidebar with icons for Home, Solutions, Learn, Settings, Compliance alerts, eDiscovery, Audit, Compliance, and Compliance Manager. The main area has a title 'New Search' and 'Audit retention policies'. It includes sections for 'Searches completed' (0), 'Active searches' (0), and 'Active unfiltered searches' (0). There are filters for 'Date and time range (UTC)\*' (Start: Dec 12, End: Dec 14), 'Activities - friendly names' (Modified file), 'Activities - operation names' (Enter operation values, separated by commas), 'Record Types' (Select the record types to search for), 'Keyword Search' (Enter the keyword to search for), 'Admin Units' (Choose which Admin Units to search for), 'Users' (User Four, User Two, Shivani Varu), 'File, folder, or site' (Enter all or a part of the name of a file, website, o...), and 'Workloads' (SharePoint, OneDrive). At the bottom, there are 'Search' and 'Clear all' buttons, and a footer with 'Copy this search', 'Delete', 'Refresh', and search filters like 'Search name', 'Job status', 'Prog...', 'Sear...', 'Total results', 'Creation ti...', and 'Search performed by'. The status bar at the bottom right shows '0 items', 'No data available', and system icons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Audit search interface. The search query information is: Thu, 12 Dec 2024 00:00:00 GMT to Sat, 14 Dec 2024 01:00:00 GMT, filenmodified, user4@MSGSTUDENT.onmicrosoft.com, user2@MSGSTUDENT.onmicrosoft.com, Shivanivaru@MSGSTUDENT.onmicrosoft.com, SharePoint, OneDrive. The total result count is 11 items. The results table includes columns for Date (UTC), IP Address, User, Record Type, Activity, Item, Admin Units, and Details. The results show multiple entries for file modifications by users shivanivaru and user2 on various SharePoint and OneDrive items.

### 4.2 Set Up Alerts:

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

The screenshot shows the Microsoft Defender Alert policy setup screen. The left sidebar lists categories like Partners and APIs, Configuration management, Identities, Dashboard, Health issues, Tools, Email & collaboration, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, Cloud apps, and Cloud discovery. The main area is titled "New Alert Policy" and has a step-by-step wizard: "Name your alert" (selected), "Create alert settings", "Set your recipients", and "Review your settings". The "Name your alert" step is highlighted with a red border. It includes fields for "Name" (Mass File Deletion Alert), "Description" (Notifies administrators when a large number of files are deleted within a short period), "Severity" (High), and "Category" (Information governance). The "Next" button is visible at the bottom right.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Defender interface for creating a new alert policy. The left sidebar lists various alert categories like Mail flow alerts, Sensitive emails, and Suspicious activity. The main area is titled 'New Alert Policy' and is on Step 3: 'Set your recipients'. It shows a list of recipient types: Name, Sensitive, Mail Flow, CC\_Social, MIP Auto, Suspicious, Email message, Admin, and A user clicked. The 'Email recipients' section contains an input field with 'ShivaniVaru@MSGSTUDENT.onmicrosoft.com' and a 'Select users' button. A red box highlights this section. Below it is a 'Daily notification limit' dropdown set to 'No limit'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

The screenshot shows the Microsoft Defender interface for creating a new alert policy. The left sidebar lists various alert categories. The main area is titled 'New Alert Policy' and is on Step 4: 'Review your settings'. It displays the alert configuration: Name (Mass File Deletion Alert), Description (Notifies administrators when a large number of files are deleted within a short period.), Severity (High), Category (Information governance). Below this is the 'Create alert settings' section with Conditions (Activity is FileDeleted) and Scope (All users, Window 1 hour). The 'Set your recipients' section includes a question 'Do you want to turn the policy on right away?' with two options: 'No, keep it off. I will turn it on later.' and 'Yes, turn it on right away.' The 'Yes' option is selected and highlighted with a red box. At the bottom are 'Back', 'Submit', and 'Cancel' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

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

The screenshot shows the Microsoft Purview Policies page. On the left, a sidebar has 'Data Loss Prevention' selected. The main area is titled 'Policies' and contains a table of policies. One policy, 'Credit Card DLP', is highlighted with a red box and shown in a detailed view on the right. The detailed view includes sections for Status (In simulation (Searching for matches)), Simulation progress (2 match found), Email notifications (On), Description (Helps detect the presence of information commonly considered to be financial data in Canada, including bank account numbers and credit cards), Admin units (None), Locations (Exchange email - All accounts, SharePoint - All accounts, OneDrive accounts - All accounts, Teams chat and channel messages - All accounts, Devices - All accounts, Microsoft Defender for Cloud Apps, On-premises repositories), and Policy settings (Low volume of content detected Credit Card DLP, High volume of content detected Credit Card DLP). Buttons at the bottom right are 'View simulation' and 'Cancel'.

The screenshot shows the 'New insider risk policy' setup wizard. The left sidebar lists steps: 'Policy template' (selected), 'Name and description', 'Users and groups', 'Content to prioritize', 'Triggering event', 'Indicators', and 'Finish'. The main area is titled 'Name your policy' and contains fields for 'Name\*' (DLP Policy Breach Monitoring) and 'Description' (Monitors and alerts administrators on DLP policy breaches involving sensitive information). Buttons at the bottom are 'Back', 'Next', and 'Cancel'.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the 'Review settings and finish' step in the Microsoft Purview Insider Risk Management policy creation wizard. The left sidebar lists completed steps: Policy template, Name and description, Users and groups, Content to prioritize, Triggering event, Indicators, and Finish. The main pane displays the final configuration of the policy:

- Policy template:** Data leaks, [Edit policy type](#)
- Name and description:** DLP Policy Breach Monitoring, Monitors and alerts administrators on DLP policy breaches involving sensitive information, [Edit policy name and description](#)
- Users, groups and adaptive scopes:** All, [Edit users, groups and adaptive scopes](#)
- Excluded users and groups:** None, [Edit excluded users and groups](#)
- Content to prioritize:** A list of URLs including https://msgstudent.sharepoint.com/sites/iteam, https://msgstudent.sharepoint.com/sites/ITDocuments, https://msgstudent.sharepoint.com/sites/hrtteam, https://msgstudent.sharepoint.com/sites/MarketingDocuments, https://msgstudent.sharepoint.com/sites/hrannouncements, https://msgstudent.sharepoint.com/sites/itdiscussions, https://msgstudent.sharepoint.com/sites/marketinginsights

At the bottom are 'Back' and 'Submit' buttons.

This screenshot shows the 'Content to prioritize' step in the Microsoft Purview Insider Risk Management policy creation wizard. The left sidebar lists completed steps: Policy template, Name and description, Users and groups, Content to prioritize, Triggering event, Indicators, and Finish. The main pane displays the configuration:

- Content to prioritize:** A list of URLs including https://msgstudent.sharepoint.com/sites/iteam, https://msgstudent.sharepoint.com/sites/ITDocuments, https://msgstudent.sharepoint.com/sites/hrtteam, https://msgstudent.sharepoint.com/sites/MarketingDocuments, https://msgstudent.sharepoint.com/sites/hrannouncements, https://msgstudent.sharepoint.com/sites/itdiscussions, https://msgstudent.sharepoint.com/sites/marketinginsights, https://msgstudent.sharepoint.com/sites/MarketingTeam811, https://msgstudent.sharepoint.com/sites/HRDocuments, https://msgstudent.sharepoint.com/sites/marketingteam. It also includes Credit Card Number, Confidential/All Employees, Highly Confidential/All Employees, Highly Confidential/Specified People, and file extensions (.doc, .dox, .pdf, .txt, .xls, .xlsx, .csv).
- Triggering event:** DLP policy: Credit Card DLP, [Edit DLP policy](#)
- Policy indicators:** 37/107 selected, No customized thresholds, [Edit policy indicators](#)

At the bottom are 'Back' and 'Submit' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Policies page. On the left, there's a sidebar with various solutions like Insider Risk Management, Data Loss Prevention, and Compliance. The main area displays a summary of policy status: 0 Policy warnings, 0 Policy recommendations, and 1 Healthy policies. A red box highlights the "DLP Policy Breach Monitoring" section. It shows a card with details: Created by: Shivani Varu, Created on: 12/14/2024, Last edited on: 12/14/2024 7:07 AM, Last edited by: Shivani Varu. Below this, under "Policy health", it says "Healthy policy. No recommendations at this time."

This screenshot is similar to the one above but shows the "Policy settings" tab for the DLP Policy Breach Monitoring section. It includes a "Policy template" section for "Data leaks", a "User coverage" section stating "This policy is covering all active users in your org. Great job!", and a "User scope" dropdown set to "Include all users and groups (Recommended for best coverage)". There's also a "Save changes" button and a "Content to prioritize" list with "SharePoint sites" and "Sensitivity labels". A red box highlights the "Policy settings" tab and its associated content.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Policies page. On the left, there's a sidebar with various navigation options like Home, Solutions, Learn, Settings, and several compliance-related sections. The main area displays a summary of policy status: 0 Policy warnings, 0 Policy recommendations, and 1 Healthy policies. A red box highlights the 'DLP Policy Breach Monitoring' section, which includes:

- Content to prioritize:** SharePoint sites, Sensitivity labels, Sensitive Info types, File extensions, Trainable classifiers.
- Scoring:** Get alerts only for activity that includes priority content.
- Triggering thresholds:** Built-in thresholds.
- Policy indicators:** Sharing SharePoint files with people outside the organization, Sharing SharePoint folders with people outside the organization, Sharing SharePoint sites with people outside the organization, Downloading content from OneDrive, Syncing content from OneDrive (with a 'Show all' link).
- Detection options:** Download from Microsoft 365 location then exfiltrate, Downgrade or remove label then exfiltrate, Downgrade or remove label, download, then exfiltrate.

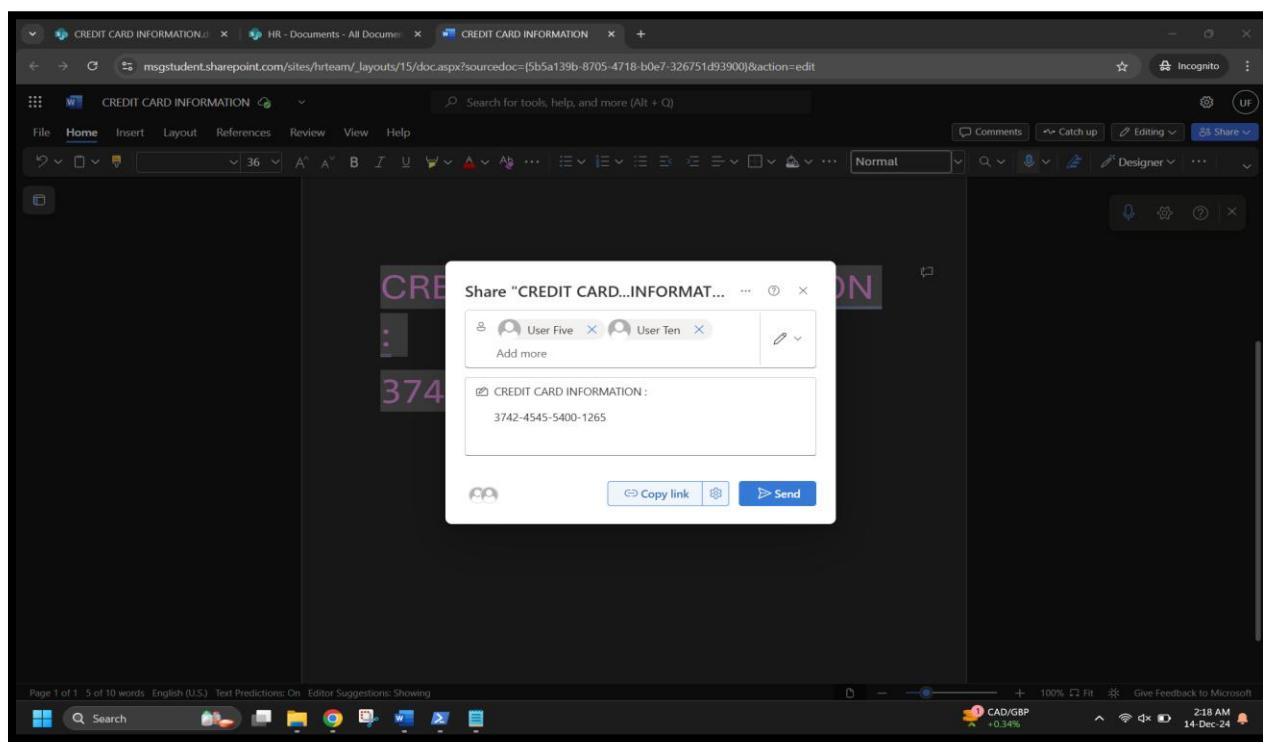
At the bottom right of the main content area are 'Edit policy' and 'Close' buttons.

This screenshot is nearly identical to the one above, showing the Microsoft Purview Policies page. The 'DLP Policy Breach Monitoring' section is highlighted with a red box. The 'Detection options' list has been modified to include:

- Download from Microsoft 365 location then exfiltrate
- Downgrade or remove label then exfiltrate
- Downgrade or remove label, download, then exfiltrate

Below this, new sections are visible: 'Cumulative exfiltration detections' (Detect when a user's exfiltration activities exceed organizational norms), 'Boosters' (Activity is above user's usual activity for that day), and 'Indicator thresholds' (Built-in thresholds). The bottom right still features 'Edit policy' and 'Close' buttons.

## Microsoft 365 Identity and Services – Enterprise Administration

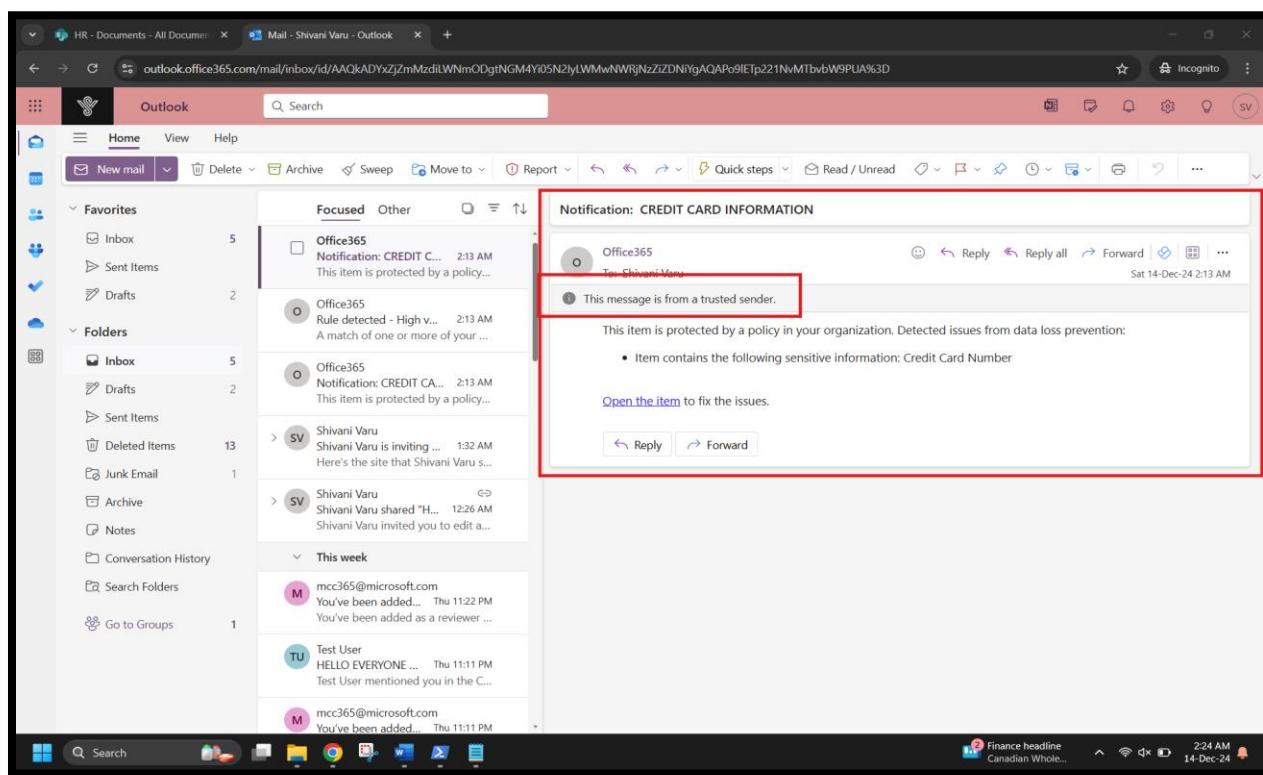


A screenshot of Microsoft Outlook. In the inbox, there is a message from "Office365" with the subject "Notification: CREDIT C...". A red box highlights this message. Another red box highlights a detailed DLP alert window that has popped up over the message. The alert window contains the following information:

- Rule detected - High volume of content detected Credit Card DLP
- This item is protected by a policy...
- Report ID: 9148a4a1-e59a-4d3a-aafa-e113dfaee5e0
- Service: SharePoint
- Matched item: <https://msgstudent.sharepoint.com/sites/hrteam/Shared%20Documents/CREDIT%20CARD%20INFORMATION.docx>
- Title: CREDIT CARD INFORMATION
- Document author: Shivan Varu <shivanvaru@msgstudent.onmicrosoft.com>
- Person who last modified document: SHIVANIVARU@MSGSTUDENT.ONMICROSOFT.COM
- Severity: High
- Condition matched: Contains sensitive information
- Rule matched: High volume of content detected Credit Card DLP
- Rule actions: NotifyUser, GenerateAlert, GenerateIncidentReport
- Policy name: Credit Card DLP
- Policy ID: 48aa450c-c282-474f-9195-4bf72abb591b
- Policy Mode: AuditAndNotify

The alert window also shows a "Sign in with a different account" button. The Outlook ribbon at the top includes Home, View, Help, New mail, Delete, Archive, Sweep, Move to, Report, Quick steps, Read / Unread, and a search bar.

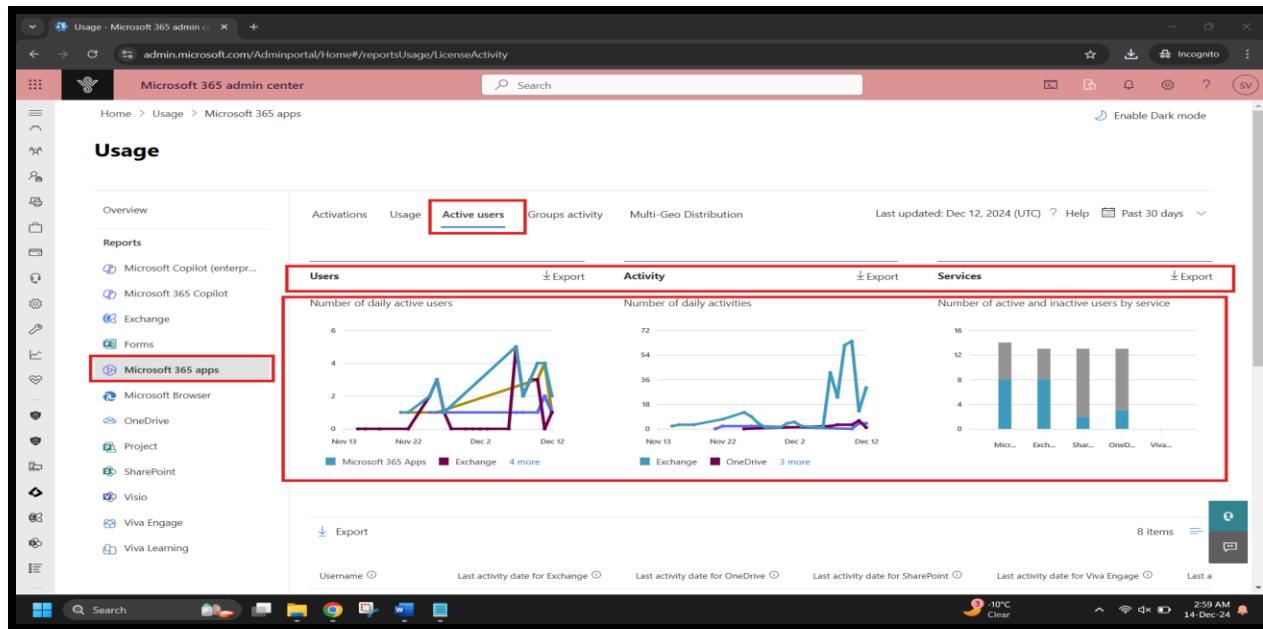
## Microsoft 365 Identity and Services – Enterprise Administration



### 4.3 Generate Usage Reports:

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

#### A. User Activity Reports



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

User Activity Reports.csv

File Home Insert Page Layout Formulas Data Review View Automate Help Acrobat

Paste B I U Alignment Fg Number Fg Styles Cells Editing Sensitivity Add-ins Analyze Data Create PDF and Share link Share via Outlook Adobe Acrobat

Clipboard Font Alignment Number Styles Cells Editing Sensitivity Add-ins Analyze Data Create PDF and Share link Share via Outlook Adobe Acrobat

POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. Don't show again Save As...

A1 Report Refresh Date User Principal Name Display Name Is Deleted Deleted On Has Exchange Has OneDrive Has SharePoint Has Skype Has Yammer Has Team Exchange OneDrive SharePoint Yammer Lync Teams Lync Exchange OneDrive Lync Share

|    | A        | B                  | C                   | D            | E          | F          | G            | H            | I              | J         | K          | L        | M        | N        | O          | P      | Q    | R        | S        |     |
|----|----------|--------------------|---------------------|--------------|------------|------------|--------------|--------------|----------------|-----------|------------|----------|----------|----------|------------|--------|------|----------|----------|-----|
| 1  | Report   | Refresh Date       | User Principal Name | Display Name | Is Deleted | Deleted On | Has Exchange | Has OneDrive | Has SharePoint | Has Skype | Has Yammer | Has Team | Exchange | OneDrive | SharePoint | Yammer | Lync | Teams    | Lync     |     |
| 2  | 08-12-24 | 27D000633E1B3B6FB  | DCEB1D07E1E01A0A2   |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    | 08-12-24 |          |            |        |      | 07-12-24 | 07-12-24 | 07- |
| 3  | 08-12-24 | AC5C513F67AA01C1F2 | B6DFC8C1466AA434DE  |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    | 07-12-24 | 07-12-24 | 07-12-24   | 07-    |      | 07-12-24 | 07-12-24 | 07- |
| 4  | 08-12-24 | 74D6B8C9C97B284    | E5D2AD241EC44CF155  |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    |          |          |            |        |      | 07-12-24 | 07-12-24 | 07- |
| 5  | 08-12-24 | DA97FA93BD3C4231   | 3B1265FB67193B8A725 |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    |          |          |            |        |      | 07-12-24 | 07-12-24 | 07- |
| 6  | 08-12-24 | 55D3005EBF049B48   | BD95AF62573B14167EF |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    |          |          |            |        |      | 26-11-24 | 26-11-24 | 26- |
| 7  | 08-12-24 | AE20BE66B6C40A02C  | BE0924A14617FF76194 |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    | 07-12-24 |          |            |        |      | 07-12-24 | 07-12-24 | 07- |
| 8  | 08-12-24 | A9B91C44AC7B6367   | 9DAE2A15DFDCC42B0   |              | FALSE      | TRUE       | TRUE         | TRUE         | FALSE          | TRUE      | TRUE       | FALSE    | 08-12-24 | 08-12-24 |            |        |      | 07-12-24 | 07-12-24 | 07- |
| 9  | 08-12-24 | BCA20605844C8723   | 5AD55D96ABF0E50647I |              | FALSE      | FALSE      | FALSE        | FALSE        | FALSE          | FALSE     | FALSE      | FALSE    | 07-12-24 |          |            |        |      |          |          |     |
| 10 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 11 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 12 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 13 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 14 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 15 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 16 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 17 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 18 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 19 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 20 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 21 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 22 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 23 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 24 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 25 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 26 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 27 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 28 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 29 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 30 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |
| 31 |          |                    |                     |              |            |            |              |              |                |           |            |          |          |          |            |        |      |          |          |     |

User Activity Reports

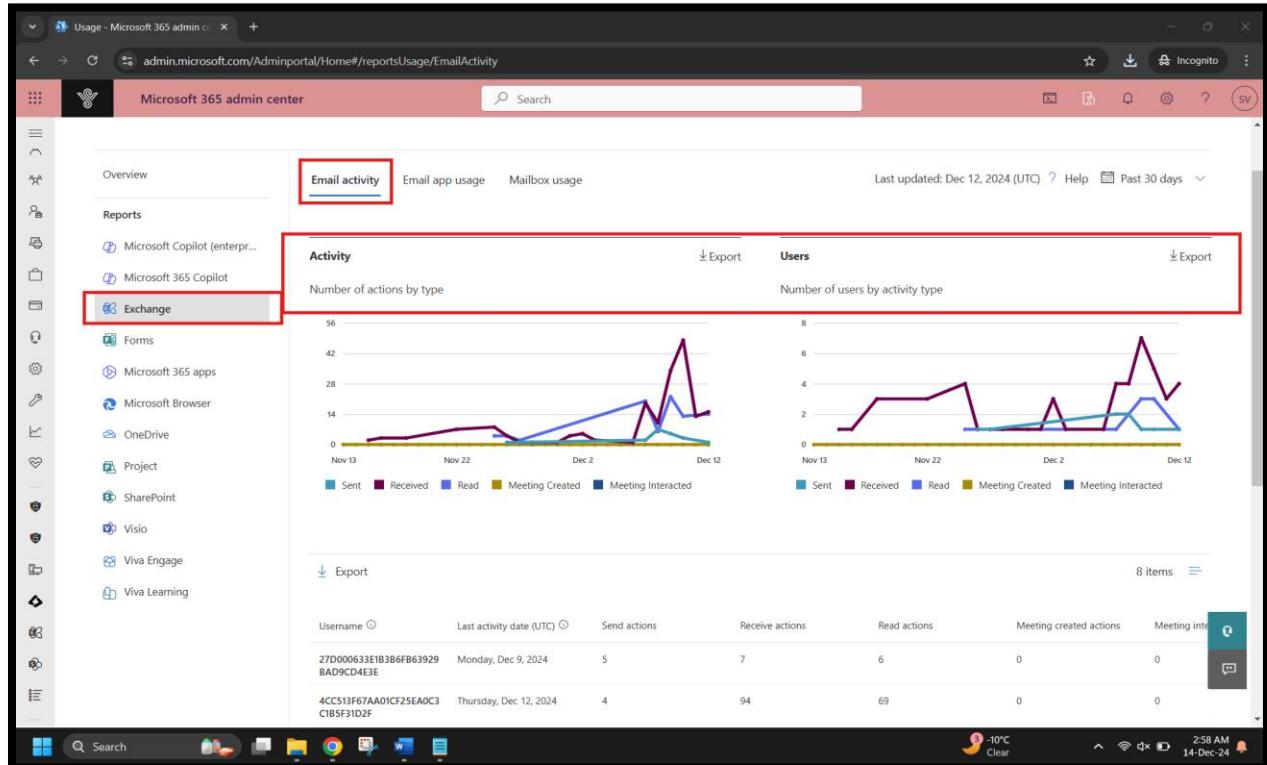
Ready Accessibility: Unavailable

Search

11°C Clear

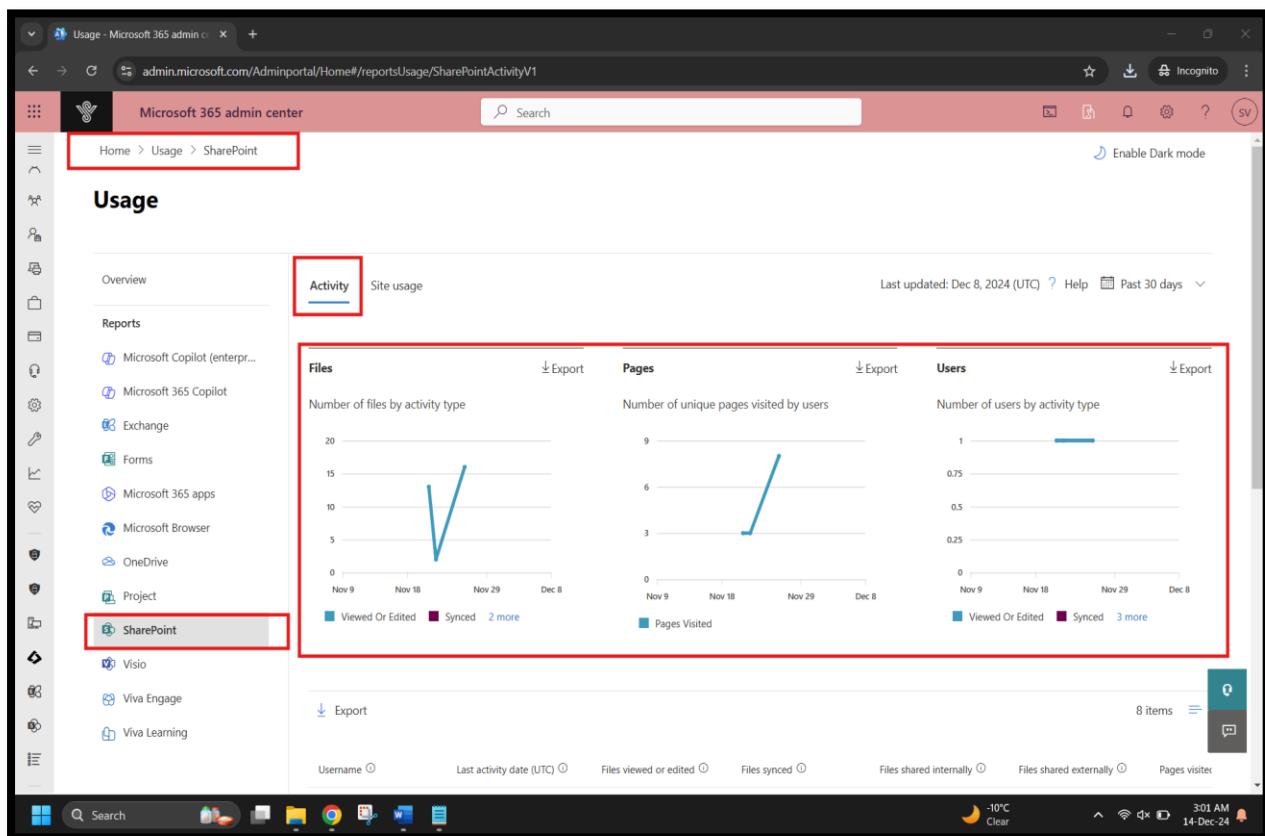
3:49 AM 14-Dec-24

## B. Email Usage Reports



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

## C. SharePoint Usage Reports



## Microsoft 365 Identity and Services – Enterprise Administration

| Report Refresh Date | User Principal Name  | Is Deleted | Deleted On | Last Activit Viewed On | Synced File Shared Int Shared Ext Visited Pg Assigned P | Report Period  |
|---------------------|----------------------|------------|------------|------------------------|---------------------------------------------------------|----------------|
| 08-12-24            | 27D000633E1B3BE6B39  | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | 4CC513F67AA1C1F25EA  | FALSE      | 26-11-24   | 30                     | 0 0 0 0 0 0                                             | 11 MICROSOF 30 |
| 08-12-24            | 74D6BBC9C9B264F5E    | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | D979A380C34231B91    | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | 55D3005EBF049484E0   | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | A20B0E66B8C400A20403 | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | A9891C44AC7B6367BD2  | FALSE      |            |                        | 0 0 0 0 0 0                                             | 0 MICROSOF 30  |
| 08-12-24            | 8CA20605844C8723D24E | FALSE      |            |                        | 0 0 0 0 0 0                                             | 30             |

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

Three ways to make a flow

Start from blank

Build a scheduled cloud flow

Flow name: Monthly Usage Report Distribution

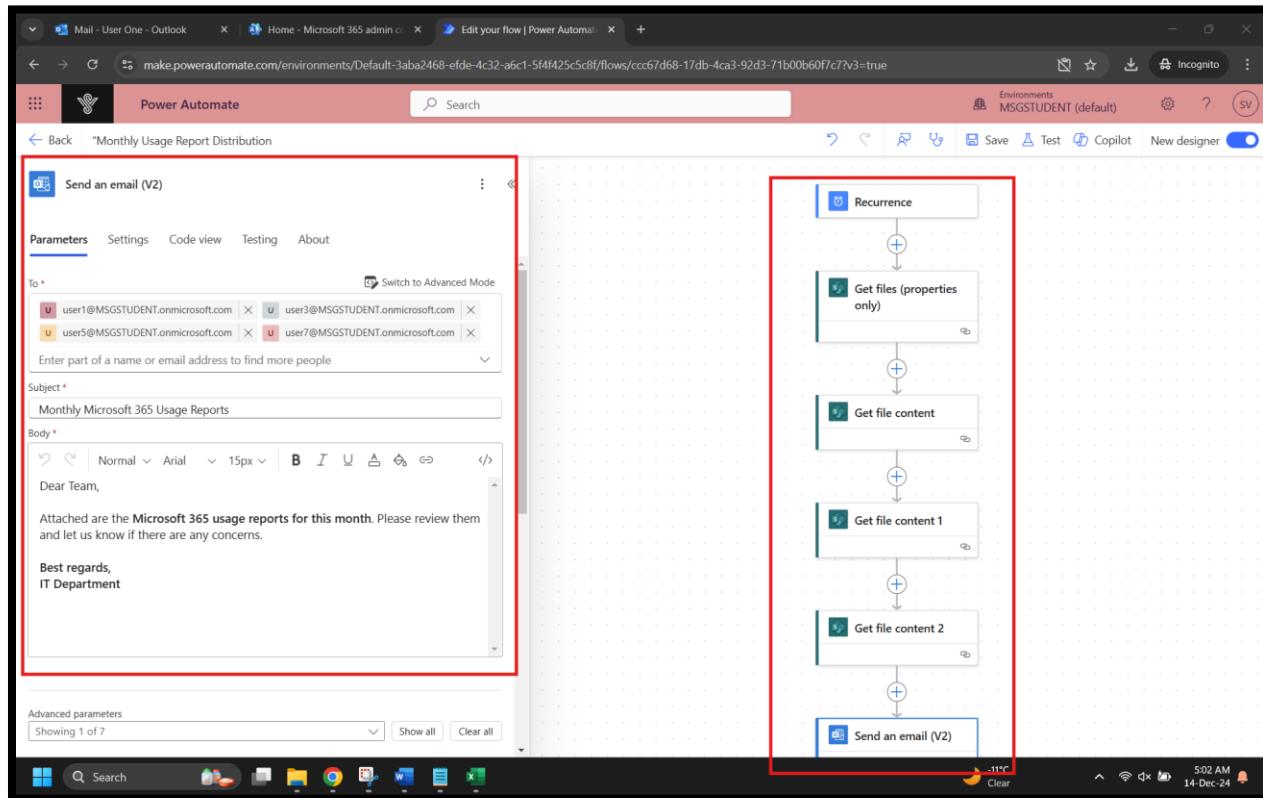
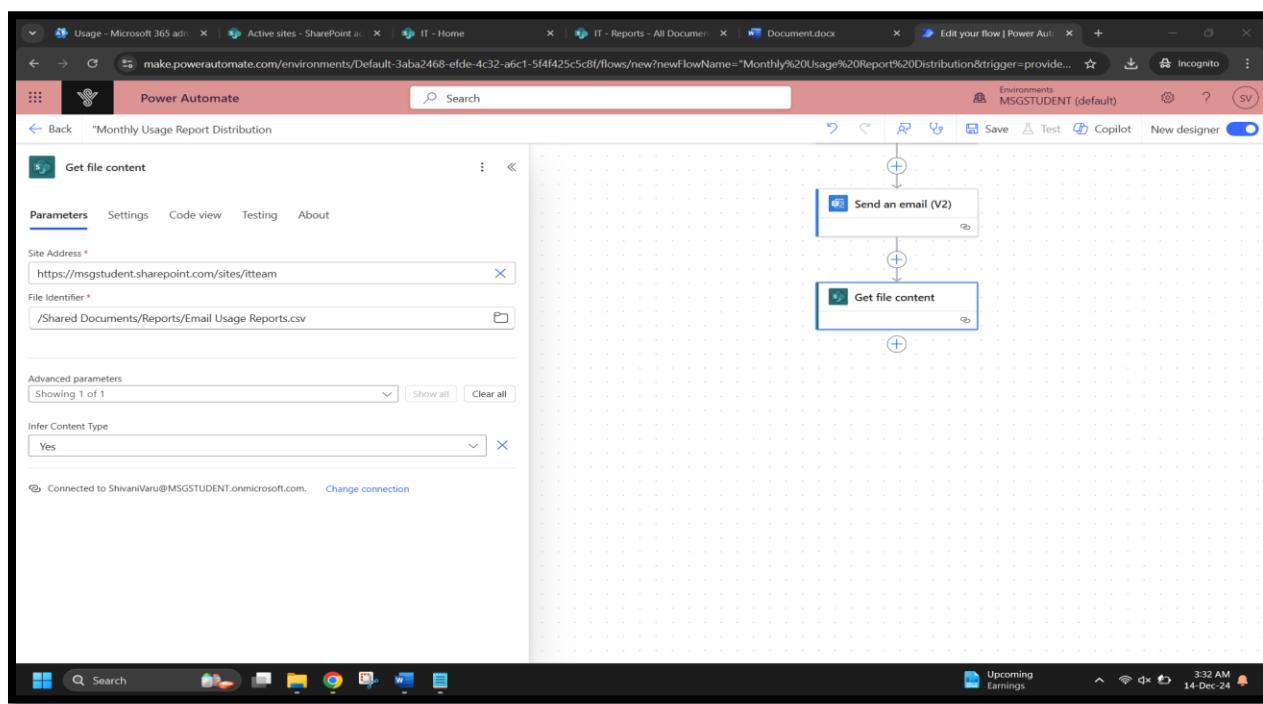
Run this flow:

- Starting: 12/14/24 at 03:00 AM
- Repeat every: 1 Month

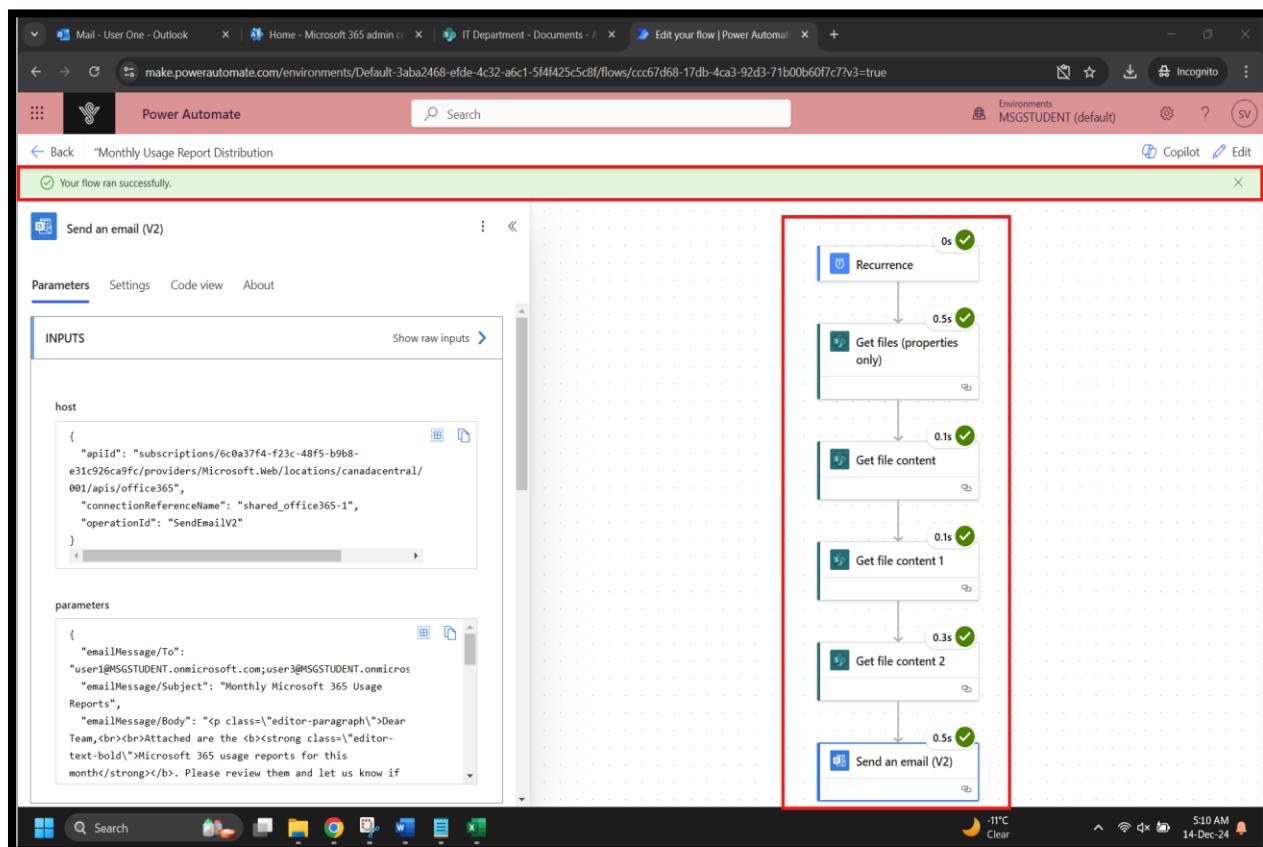
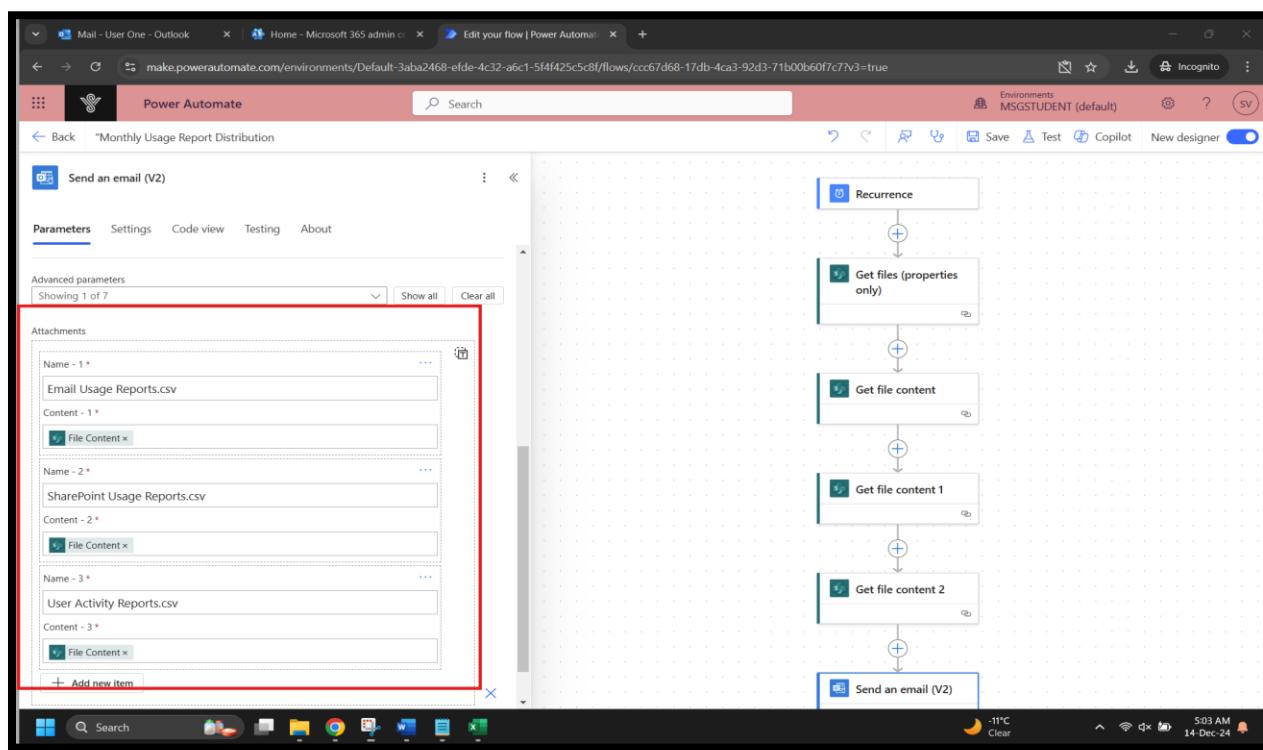
This flow will run:  
Every month

Skip Create Cancel

## Microsoft 365 Identity and Services – Enterprise Administration

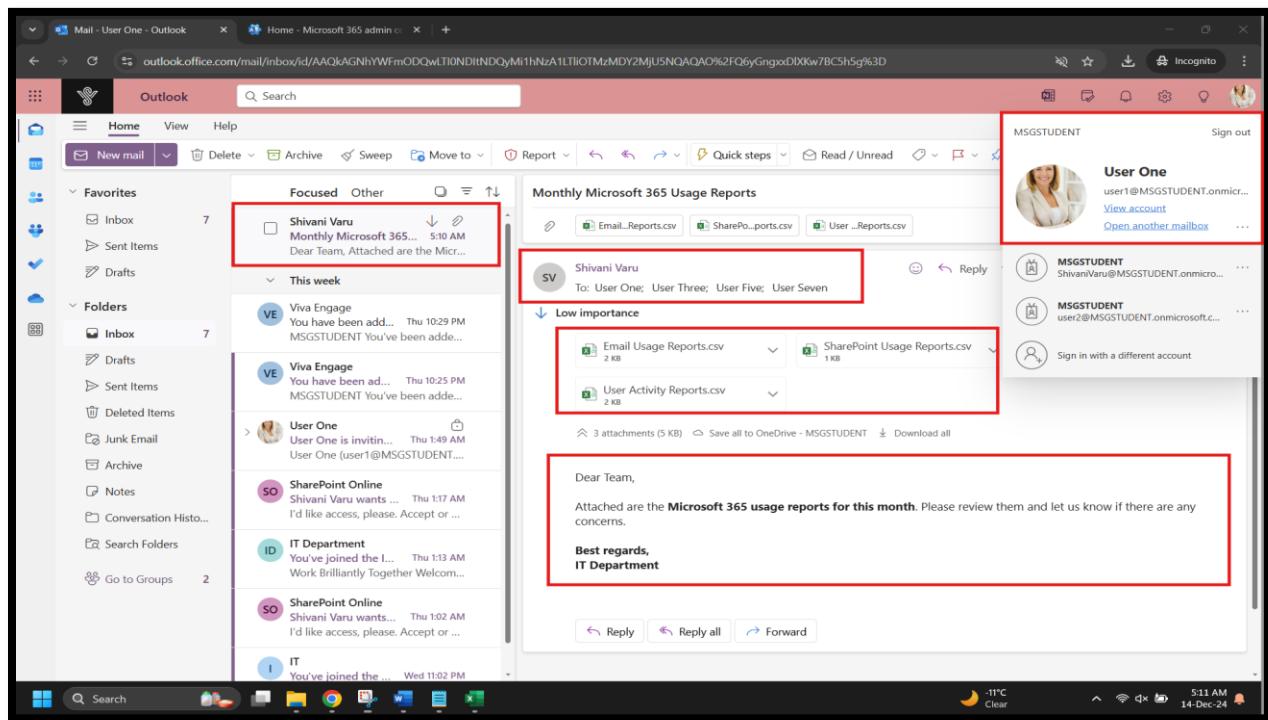


## Microsoft 365 Identity and Services – Enterprise Administration



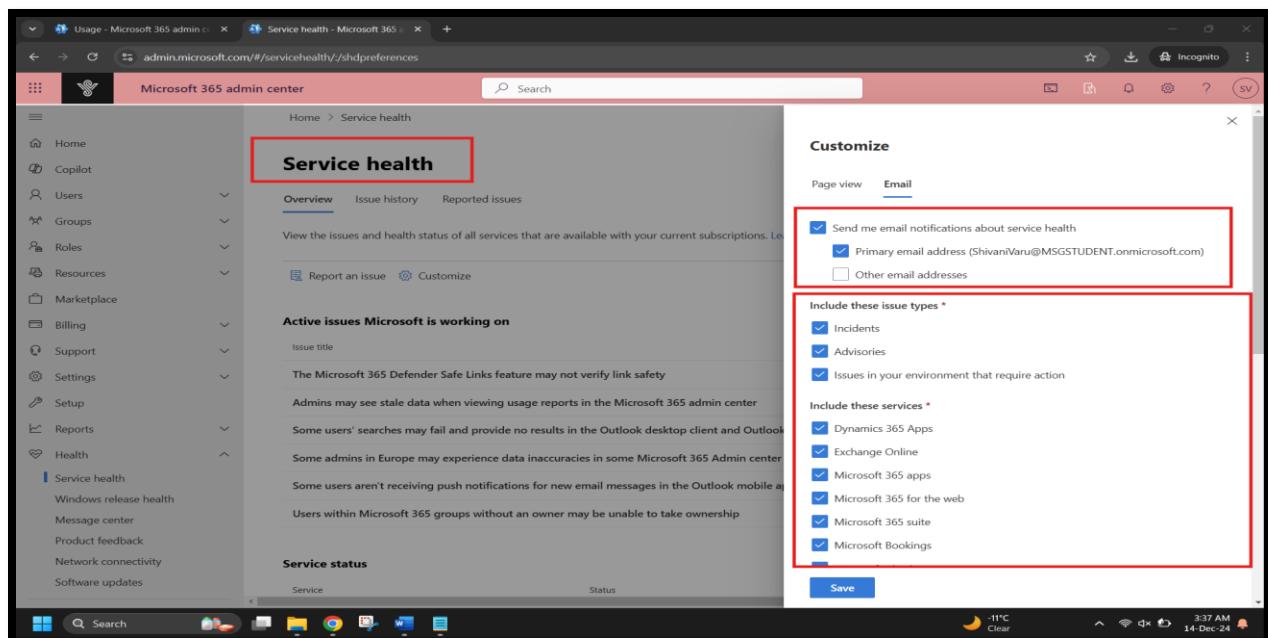
## Microsoft 365 Identity and Services – Enterprise Administration

[ Screenshot : User one ( IT manager of TechSolution inc) Receive monthly reports from administrators automatically via power automate in email ]



### 4.4 Implement and Monitor Service Health:

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



## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Admin Center with the 'Service health' page open. A 'Customize' overlay is displayed on the right side, containing settings for email notifications and issue types. A red box highlights the 'Customize' button and the 'Changes saved' message.

The screenshot shows the Microsoft 365 Admin Center with a specific service health alert highlighted. The alert title is 'Some users' searches may fail and provide no results in the Outlook desktop client and Outlook on the web'. The alert details section includes user impact, scope of impact, root cause, and updates. A red box highlights the alert title.

## Microsoft 365 Identity and Services – Enterprise Administration

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

The screenshot shows the Microsoft 365 Service Health dashboard. On the left, a navigation menu is open, with the 'Health' section expanded, specifically the 'Service health' item. A red box highlights this selection. The main content area is titled 'Service health' and contains three tabs: 'Overview' (selected), 'Issue history', and 'Reported issues'. Below these tabs, a message encourages users to view the status of all services. Under the 'Overview' tab, there's a section titled 'Active issues Microsoft is working on' with a table. Another red box highlights this table. The table has columns for 'Issue title', 'Issue type', 'Affected service', and 'Updated'. It lists several issues, such as 'The Microsoft 365 Defender Safe Links feature may not verify link safety' (Advisory, Microsoft Defender XDR, Dec 13, 2024) and 'Admins may see stale data when viewing usage reports in the Microsoft 365 admin center' (Advisory, Microsoft 365 suite, Dec 13, 2024). At the bottom of the dashboard, there's a 'Service status' section with a table showing various Microsoft services and their current status as 'Healthy'.

This screenshot shows the same Microsoft 365 Service Health dashboard as the previous one, but with a different focus. The 'Service status' section is highlighted with a large red box. This section displays a list of Microsoft services and their current status. All services listed are marked as 'Healthy'. The services include Dynamics 365 Apps, Microsoft 365 apps, Microsoft 365 for the web, Microsoft Bookings, Microsoft Clipchamp, Microsoft Entra, Microsoft Forms, Microsoft Intune, Microsoft Power Automate, Microsoft Power Automate in Microsoft 365, Microsoft Purview, Microsoft Stream, Microsoft Teams, Microsoft Viva, and Mobile Device Management for Office 365.

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Service Health - Reported issues page. The URL is [admin.microsoft.com/#/servicehealth/reportedissues](https://admin.microsoft.com/#/servicehealth/reportedissues). The page title is "Service health". The navigation bar includes "Overview", "Issue history", and "Reported issues" (which is underlined, indicating it is the active tab). A search bar is at the top right. The main content area displays a message: "No issues reported in the last 30 days. If you reported issues recently but you don't see them here, try refreshing the page." Below this message, there is a table header with columns: Service, Category, Significant impact, Reported by, State, and Username. The table body is empty, showing "0 items". There are buttons for "Report an issue", "Export", and "Customize". A filter and change view button are also present. The left sidebar shows the "Service health" section under the "Health" category. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.