Student Lab Manual
MS101.2x: Microsoft 365 Compliance Management

Lab Scenario

You are the system administrator for Adatum Corporation, and you have Office 365 deployed in a virtualized lab environment. In this lab, you will set up a Microsoft 365 tenant account, prepare an Office 365 ProPlus managed installation, manage user-driven Office 365 ProPlus installations, manage centralized Office 365 ProPlus installations, and deploy and configure Office Telemetry components.

There are seven exercises in this lab, each of which contains one of more tasks. For a successful outcome to the lab, the exercises and their corresponding tasks must be completed in order. The seven exercises include:

- Exercise 1: Initialize Compliance in Your Organization
  - Task 1 – Obtain your Office 365 credentials
  - Task 2 - Create the tenant account
  - Task 3 – Create users and groups for the trial tenant
  - Task 4 – Configure MDM auto-enrollment

- Exercise 2: Configure Retention Tags and Policies
  - Task 1 – Activating In-Place Archiving
  - Task 2 – Create an MRM retention tag and policy in the Exchange Admin Center
  - Task 3 – Create a retention policy in the Security and Compliance Center
  - Task 4 – Create a DLP policy with custom settings

- Exercise 3: Configure AIP and WIP
  - Task 1 – Configure Azure Information Protection
  - Task 2 - Configure Windows Information Protection

- Exercise 4: Testing DLP Policies
  - Task 1 – Use Archiving (MRM Retention Tags)
  - Task 2 – Send sensitive emails (DLP policy)

- Exercise 5: Using Azure Information Protection
    - Task 1 – Use AIP on a client
    - Task 2 – Verify AIP policy

- Exercise 6: Using Windows Information Protection
    - Task 1 – Use WIP

- Exercise 7: Investigate your Microsoft 365 Data
    - Task 1 – Perform a content search for deleted emails
    - Task 2 – Create an eDiscovery case

WARNING – Be prepared for UI changes

Given the dynamic nature of Microsoft cloud tools, you may experience user interface (UI) changes that were made following the development of this training content that do not match up with lab instructions presented in this lab manual.

The Microsoft Learning team will update this training course as soon as any such changes are brought to our attention. However, given the dynamic nature of cloud updates, you may run into UI changes before this training content is updated. **If this occurs, you will have to adapt to the changes and work through them in the labs as needed.**

Exercise 1: Initialize Compliance in your organization

Task 1 - Obtain Your Office 365 Credentials

Once you launch the lab, a free trial tenant will be automatically created for you to access Azure in the Microsoft Virtual Lab environment. This tenant will be automatically assigned a unique user name and password. You must retrieve this user name and password so that you can sign into Azure within the Microsoft Virtual Lab environment.

1. On the **XtremeLabs Online** menu bar at the top of the screen, click on the **Files** drop-down arrow.
2. Click on **O365 Credentials**. A window will open with your credentials.
3. This is the user name and password you will need to sign in to Azure. Keep this page open as you will need the information later.
4. When the lab directs you to sign in to the Azure portal at **https://portal.azure.com,** you will sign in using the credentials you obtained in this task.

Task 2 - Create the tenant account

Perform the following steps to create your Microsoft 365 Enterprise E5 tenant account:

1. Open the Microsoft Edge browser and go to https://aka.ms/compliancelab.
2. In the middle of the page, below the **Contact sales** area, click **Free trial.**
3. On the **Welcome, let's get to know you** page, type or select the following for your lab environment:
    a. Country/region: **United States**
    b. First name: **Ramiro**
    c. Last name: **Armenta**
    d. Business email address: Use your own personal email address
    e. Business phone number: Use your business phone number or, if you are outside of the United States, use **0123456789**
    f. Company name: **Adatum Corp.**
    g. Organization size: **50-249 people**
4. Click **Next**.
5. In the **Create your user ID** page, you must create a unique domain for the Company name to use in the course. Type a unique Microsoft 365 tenant name as outlined in the introduction of this lab manual.
    a. Username: **admin**
    b. Yourcompany: **AdatumXXXXXX** (where XXXXXX is your unique tenant name)
    c. Create password: **Pa$$w0rd**
    d. Confirm password: **Pa$$w0rd**
6. When all fields are valid, click **Create my account**.
7. On the **Prove. You're. Not. A. Robot.** page, you must confirm your identity by using your mobile phone.
    a. Select **Text me** (if it's not already selected).

   b. From the drop-down box, select the code for the country/region your phone is available.
   c. In the **Phone number** box, type your correct mobile phone number.
   d. Click **Text me**.
   e. Wait till the text message arrives and type the code to the **Enter your verification code** field.
   f. Click **Next**.
8. Wait till your Microsoft 365 E5 trial tenant is provisioned and write down the address below **Your user ID**, which is your ID to login to your tenant.
9. Click **Start Setup**.
10. Leave the setup wizard with a click on **Exit and continue later**.
11. On the Microsoft 365 Admin Center click on **Skip** to close the tour screen.
12. Click on your browsers address bar and navigate to: https://aka.ms/emse5trial.
13. Below the **It looks like you already have an account** headline, click at **Yes, add it to my account**.
14. On the **Check out** screen, you are ask to **confirm your order**. Click **Try now.**
15. You will see an **order receipt** summary screen. Click **Continue** to finish the process.

You have completed the steps to provision your Microsoft 365 E5 tenant account and added the EMS E5 licenses. Leave your web browser on Ramiro's Admin center page and proceed to the next task.

Task 3 - Create Users and Groups for the Trial Tenant

In this exercise you will create two users, required for exercises that will be covered later in this lab environment.

You should still be logged in as Ramiro Armenta and see the Admin Center page. Perform the following steps to create users for the lab exercises:

1. Click on **Groups** on the left tab and select **Groups** from the menu below.
2. Click on **(+) Add a group** to open the right **New group** pane.
3. Fill all the fields to create the **WIP Users** group:
   a. Type **Mail-enabled security**
   b. Name **WIP Users**
4. Create the group by clicking on **Add**.
5. Click **Close**.
6. Click on **Users** on the left tab and select **Active users**.
7. Click on **(+) Add a user** to open the right **New user** pane.
8. Fill all the fields to create the first user **Marguerite Ortiz**:
   a. First name: **Marguerite**
   b. Last name: **Ortiz**
   c. Display name: **Marguerite Ortiz**
   d. Username: **Marguerite**
   e. Domain: Keep the default selection.
   f. Location: Preselected with your tenant's location.
9. Select the Password area.
   a. Select **Let me create the password** and type **Pa$$w0rd** into the text field.

    b. Deselect **Make this user change their password when they first sign in**.
10. Select the **Product licenses** area to open the licensing selection.
    a. Click on the slider for **Microsoft 365 Enterprise E5.**
    b. Click on the slider for **Enterprise Mobility + Security E5.**
11. Create the user by clicking **Add** on the lower end of the right panes screen.
12. Click **Add another user** below Next steps.
13. Fill all the fields to create the second user **Judy Wyatt**:
    a. First name: **Judy**
    b. Last name: **Wyatt**
    c. Display name: **Judy Wyatt**
    d. Username: **Judy**
    e. Domain: Keep the default selection.
    f. Location: Preselected with your tenant's location.
14. Select the Password area.
    a. Select **Let me create the password** and type **Pa$$w0rd** into the text field.
    b. Deselect **Make this user change their password when they first sign in**.
15. Select the **Product licenses** area to open the licensing selection.
    a. Click on the slider for **Microsoft 365 Enterprise E5**
    b. Click on the slider for **Enterprise Mobility + Security E5**
16. Create the user by clicking **Add** on the lower end of the right panes screen.
17. Click **Send email and close** to receive the login data via email.
18. Go back again to **Groups** on the left tab and select **Groups** from the menu below.
19. Click on the group **WIP Users** and click on **Edit** in the **Members** row.
20. Click on **(+) Add members** and select **Marguerite Ortiz** and **Judy Wyatt**. Click **Save**.
21. Click **Close** three times.

You have now created three users with Microsoft 365 E5 and EMS E5 licenses assigned. Leave your web browser on Ramiro's Admin center page, in the Users section, and proceed to the next exercise.

Task 4 – Configure MDM auto-enrollment

In this exercise you will activate the MDM auto-enrollment for new devices in your tenant. This feature will be required for the Windows Information Protection exercise later.

Perform the following steps:

1. Open the Microsoft Edge browser and go to https://portal.azure.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account (replace the XXXXXX with the corresponding attribute from your O365 Credentials) using a password of **Pa$$w0rd**.
3. On the **Welcome to Microsoft Azure** page, click **Maybe later**.
4. Click on **All Services**, type Azure Active Directory and click on **Azure Active Directory**.
5. Click on **Mobility (MDM and MAM)** from Manage on the left-side pane.
6. Click on **Microsoft Intune**.

7. In the **MDM User scope** section, click **Some** and click on **Select groups** below.
8. Select **WIP Users** from the right-side pane and click **Select**.
9. Click on **Restore default MDM URLs** to ensure the correct URLs are set.
10. Click **Save** on the top menu.
11. Click on **All Services**, type Intune and click on **Intune**.
12. Click on **Device enrollment** from the left pane.
13. You are requested to **Choose MDM Authority**. Select **Intune MDM Authority** and click **Choose**.

You have now activated the auto-enrollment feature for all devices of users, that are a member in the Azure AD group WIP Users. Proceed with the next exercise.

Exercise 2 – Configure Retention Tags and Policies

Task 1 – Activating In-Place Archiving

Activate the archive mailboxes for the two users in your tenant. If any dialogs of the following instructions are missing, your test tenant is probably not completely provisioned yet. Wait for some time till the dialogs appear and continue the step you are working on.

To activate the in-place archiving in the Security & Compliance Center, perform the following steps:

1. Open the Microsoft Edge browser and go to https://protection.microsoft.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. Wait a moment when you visit the Security & Compliance Center for the first time and reload the page after one or two minutes.
4. In the Security & Compliance Center select **Data Governance** from the left pane and click on **Archive**.
5. Select **Judy Wyatt** and wait till the details pane on the right side is ready.
6. Below **Archive mailbox: disabled**, click **Enable**.
7. A warning message is displayed, that tells you the default MRM retention policy action will apply. Click **Yes** to acknowledge the warning.
8. Select **Marguerite Ortiz** and wait till the details pane on the right side is ready.
9. Below **Archive mailbox: disabled**, click **Enable**.
10. A warning message is displayed, that tells you the default MRM retention policy action will apply. Click **Yes** to acknowledge the warning.

You have activated the archive mailbox for the users **Judy Wyatt** and **Marguerite Ortiz**. Leave your web browser on Ramiro's Security & Compliance Center page and proceed to the next exercise.

Task 2 – Create an MRM retention tag and policy in the Exchange Admin Center

In this exercise, you will create a MRM retention tag and add it to a new MRM retention policy. Then you will change the retention policy for the two users with enabled archive mailboxes.

Perform the following steps to configure MRM retention:

1. Open a new Edge browser windows or select the address bar in your browser and go to https://admin.microsoft.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. Select **… Show more** from the left pane.

4. Select **Admin centers** and click on **Exchange**.
5. In the Exchange admin center click on **compliance management** from the left pane.
6. On the menu bar on the top of the page, click on the **retention tags** tab.
7. On the toolbar, click the **(+)** sign. In the drop-down menu, select **applied by users to items and folders (personal)**.
8. In **new tag applied by users to items and folders (personal)** window, under **Name**, type **3 Years Move – Archive after three years**.
9. Under **Retention Action**, select the **Move to Archive** option.
10. Under **Retention period**, select the **When the item reaches the following age (in days)** option, and type **1095** in the retention period field.
11. Click **Save**.
12. On the menu bar on the top of the page, click on the **retention policies** tab.
13. On the toolbar, click the **(+)** sign.
14. In **new retention policy** window, under **Name**, type **Office Retention Policy**.
15. Below **Retention tags**, click the **(+)** sign.
16. Click the tag starting with **3 Years Move** (the column width will truncate the displayed name), click **add ->**, and then click **OK**.
17. On the **new retention policy** window, click **Save**.
18. In the Exchange Admin Center, in the left-hand column, click on **recipients**.
19. In the list of recipient mailboxes, select **Marguerite Ortiz** and then click on the **pencil icon** in the toolbar to edit the properties of Marguerite's mailbox.
20. In the **Marguerite Ortiz** properties window, click on **mailbox features**.
21. On the Warning dialog, click **Ok**.
22. Click the drop-down arrow in the **Retention policy** field and select **Office Retention Policy**.
23. Click on **Save.**
24. In the list of recipient mailboxes again, select **Judy Wyatt** and then click on the **pencil icon** in the toolbar to edit the properties of Judy's mailbox.
25. In the **Judy Wyatt** properties window, click on **mailbox features**.
26. On the Warning dialog, click **Ok**.
27. Click the drop-down arrow in the **Retention policy** field and select **Office Retention Policy**.
28. Click on **Save.**

You have now created a new retention tag, assigned it to a retention policy and changed the default retention policy of Marguerite and Judy. Leave your web browser open and proceed to the next exercise

Task 3 – Create a Retention Policy in the Security and Compliance Center

In this lesson you will create a retention policy in the Security & Compliance Center to preserve all content of Exchange mailboxes for 7 years.

Perform the following steps:

1. Open a new Edge browser window or select the address bar in your browser and go to https://protection.microsoft.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. In the Security & Compliance Center select **Data Governance** from the left pane and click on **Retention**.
4. Click on **(+) Create** to open the wizard for creating a new retention policy.
5. On the first page **Name for policy**, type **Exchange Preservation** in the **Name** field and click **Next**.
6. On the settings page, change the Retain the content based on **when it was created** to **when it was last modified**. Click **Next**.
7. Select **Let me choose specific locations.**
8. Deselect all sliders except of **Exchange email** on the Choose locations page. Click **Next**.
9. Click **Create this policy** to finish the wizard.

You have now created a retention policy that preserves all Exchange Online mailbox from deletion for 7 years after the last modification. Leave your web browser on Ramiro's Security & Compliance Center page and proceed to the next exercise.

Task 4 – Create a DLP policy with custom settings

In this lesson you will create a Data Loss Prevention policy in the Security & Compliance Center to protect sensitive data from being shared by users.

Perform the following steps:

1. Open a new Edge browser window or select the address bar in your browser and go to https://protection.microsoft.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. In the Security & Compliance Center select **Data loss prevention** from the left pane and click on **Policy**.
4. Click on **(+) Create a policy** to open the wizard for creating a new data loss prevention policy.
5. On the template screen, select **Custom** and **Custom policy**. Click **Next**.
6. Type **IP Address DLP Policy** in the **Name** field and **Protect IP addresses from being shared** to the **Description** field. Click **Next**.
7. Select **All locations in Microsoft 365. Includes content in Exchange email and OneDrive and SharePoint documents.** on the next screen and click **Next**.
8. On the Policy settings page, the option **Find content that contains:** needs to be selected.
9. Click on **Edit** to add sensitive data types.
10. Click on **Add** and select **Sensitive info types**.
11. Click on **(+) Add** again.
12. Type into the search field **Address** and wait till the search results are displayed.
13. Select **IP Address** from the Sensitive information types.

14. Click **Add** and **Done** on the next screen.
15. Check the box on top of the page and make sure, **Any of these** is selected.
16. Click on **Save**.
17. Check if the **Detect when this content is shared:** box is selected.
18. Check if the **only with people inside my organization** from the dropdown list is selected.
19. The sensitive information types have now been added. Click **Next**.
20. On the next screen, check that **Detect when content that's being shared contains** is selected.
21. Change the number from **10** instances of the same sensitive info type to **2** and click **Next.**
22. Turn the policy on by selecting **Yes, turn it on right away**.
23. Click **Next**.
24. Check the configuration on the Review your settings page again and click **Create**.

You have now created a DLP policy that informs your users, if they want to share content that contains IP addresses. Leave your web browser on Ramiro's Security & Compliance Center page and proceed to the next exercise.

Exercise 3 – Configure AIP and WIP

Task 1 – Configure Azure Information Protection

In this exercise you will create an AIP label and add it to the default policy.

Perform the following steps:

1. Open a new Edge browser window or select the address bar in your browser and go to https://portal.azure.com/.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. If you visit the Azure Portal for the first time, you need to cancel the tour by clicking on **Maybe later**.
4. Click on **All Services**, type **Azure Information Protection** and click it.
5. Click on **Labels** from Classification.
6. Click **Add a new label** on the bottom
7. On the new page, configure the following:
    a. Enabled **On**
    b. Label display name **PII**
    c. Description **Documents, Files and emails with PIIs**
    d. Color **Black**
    e. Set permissions for documents and emails containing this label **Protect**
        i. On the Protection page on the right side, select **Set user-defined permissions (Preview)** and click **Ok**.
    f. Documents with this label have a header **Off**
    g. Documents with this label have a footer **Off**
    h. Documents with this label have a watermark **On**
        i. Watermark text: **Personal Identifiable Information**
        ii. Watermark font size: **Auto**
        iii. Watermark font name: **Default**
        iv. Watermark color: **Black**
        v. Watermark layout: **Diagonal**
    i. Click **Save** in the upper left corner.
8. You are asked if you are sure to save the changes. Click **Ok** to answer the prompt.
9. Click on **Policies** from Classification.
10. Click on the **Global** policy to edit it.
    a. Below the list of labels, click on **Add or remove labels**.
    b. From the right-side menu, select **PII** and click **Ok**.
    c. Also go down to **Users must provide justification to set a lower classification label, remove a label, or remove protection** and switch it to **On**.
    d. Click **Save** in the upper left corner.
11. You are asked if you are sure to save the changes. Click **Ok** to answer the prompt.

12. Close the Policies windows by clicking the **X** in the upper right corner.

You have now created a new label and added it to the default policy, valid for all users of your tenant. Leave your web browser on Ramiro's Azure Portal page and proceed to the next exercise.

Task 2 – Configure Windows Information Protection

In this lesson you will create a WIP policy and assign it to your WIP Users Azure AD group.

You are still signed in as Ramiro and on the Azure Portal page. Perform the following steps:

1. Click on **All Services**, type **Mobile** and click on **Mobile apps**.
2. Click on **App protection policies** from Manage on the left side.
3. Click **(+) Add a policy** from the top menu.
4. On the Add a policy screen, type or select the following:
    a. Name: **WIP Client Protection**
    b. Description: <empty>
    c. Platform: **Windows 10**
    d. Enrollment state: **With enrollment**
    e. Protected apps: Click **Add apps**, select **Office-365-ProPlus-1708-Allowed.xml** and click **Ok**. On the Protected apps screen, click **Ok** again.
    f. Exempt apps: <none>
    g. Required settings: **Block**
    h. Advanced settings: **Don't change the default values**
5. Click **Create** on the bottom of the screen.
6. On the **Mobile apps - App protection policies** click on the newly created policy.
7. Click on **Assignments** from Manage.
8. On the next screen, click on **Select groups to include** from the Include tab.
9. Select the **WIP Users** group from the list and click **Select** on the bottom of the screen.

You have now created a WIP policy (App protection policy for Windows) that is applied to any User with an MDM enrolled device in Intune. Leave your web browser on Ramiro's Azure Portal page and proceed to the next exercise.

Exercise 4 – Testing DLP Policies

In this lab module you are accessing the clients for the first time. Do not configure the client in advance, because it is enrolled in MDM when configuring the client for the first time, which is required for the following WIP exercise.

Task 1 - Use Archiving (MRM Retention Tags)

In this exercise, you will send an email from **Ramiro Armenta** to **Marguerite Ortiz**. You will then log into Microsoft 365 as **Marguerite**, locate the email in her Inbox, and then assign the email a custom retention policy that you create.

Perform the following steps:

1. Open a new Edge browser window or select the address bar in your browser and go to https://outlook.office365.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. If you approach the site for the first time, you will be asked for your language setting and your time zone:
    a. From the Language dropdown select **English (United States)**
    b. From the Time zone dropdown select your preferred time zone.
4. Click **Save**.
5. On the Outlook on the web main screen, click on **(+) New** in the upper left part of the screen.
6. The forms for a new email open. Type the following:
    a. To: Write down **Marguerite** and select her email address from the dropdown list
    b. Add a subject: **Archive Test**
    c. Add a message or drop a file here: **Use this email to test archiving.**
7. Click **Send** in the lower left part of the screen.
8. Switch to the client system BER-CL01 and login as **Marguerite Ortiz (marguerite@AdatumXXXXXX.onmicrosoft.com)**, with the password **Pa$$w0rd**.
9. Open a new Edge browser window or select the address bar in your browser and go to https://outlook.office365.com.
10. If you are not automatically signed into Microsoft 365 as **Marguerite Ortiz**, then on the Microsoft 365 sign-in page, sign in to **Marguerite's marguerite@AdatumXXXXXX.onmicrosoft.com** account using the password **Pa$$w0rd**.
11. If you approach the site for the first time, you will be asked for your language setting and your time zone:
    a. From the Language dropdown select **English (United States)**
    b. From the Time zone dropdown select your preferred time zone.
12. Click **Save**.
13. In Marguerite's Inbox, you should see the email message that Ramiro just sent to Marguerite.

Note: Back when you created Marguerite's mailbox in the Lab 2, you enabled her mailbox for archiving, and you assigned the retention policy titled **Office Retention Policy** to her mailbox. This policy included the **3 Year Move – Archive after three years** retention tag. While this policy will be applied by the Managed Folder Assistant to all the received messages in Marguerite's mailbox, she has decided to override this policy for the message that she just received from Ramiro. Marguerite has decided to archive it sooner than 3 years. She will do this by creating a custom, personal retention policy and assigning it a retention tag that archives messages after 1 year.

14. Perform the following steps to create a custom retention policy:
    c. Click on the **Settings** icon in the upper right corner of the toolbar (the gear-shaped icon).
    d. In the drop-down menu that appears, scroll to the bottom of the menu, and under the **Your app settings** section, click on **Mail**.
    e. In the **Options** pane that appears on the left-hand side of the screen, under **Mail Automatic processing**, click on **Retention policies**.
    f. Click on the **(+)** to add a custom retention policy.
    g. Select the **Personal 1 year move to archive** retention tag and click **Add**.
    h. Click **Save** at the top of the screen.
15. Perform the following steps to assign the custom retention policy to a selected email message:
    i. In the **Options** pane, click on **Options** in the top left corner to return to Marguerite's mailbox.
    j. In the **Inbox**, right click on the message that she received from Ramiro with the subject: **Archive Test**.
    k. In the menu that appears, click on **Assign Policy**. In the Assign Policy menu, under Archive Policy, select **Personal 1 year move to archive (1year).**

This personal retention policy will now override the parent folder policy for this specific message, which will be moved to Marguerite's In-Place archive mailbox after 1 year rather than 3 years.

Task 2 - Send sensitive emails (DLP Policy)

Perform the following steps:

In Lab 2, Exercise 1, Task 4 you created a new DLP policy that searches for sensitive information of the type **IP Address** at all places of your tenant.

In this exercise, you will send an email with sensitive information from **Ramiro Armenta** to **Marguerite Ortiz**.

Switch to the management system and perform the following steps:

1. Open a new Edge browser window or select the address bar in your browser and go to https://outlook.office365.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. On the Outlook on the web main screen, click on **(+) New** in the upper left part of the screen.

4. The forms for a new email open. Type the following:
    a. To: Write down **Marguerite** and select her email address from the dropdown list
    b. Add a subject: **DLP Policy Test**
    c. Add a message or drop a file here: **I will hack this IP address: 192.168.0.1**
5. Wait a moment, till the message is saved as a draft.
6. You will see a policy tip above your message fields.
7. Click **Send** in the lower left part of the screen.
8. Write a second message, by clicking on **(+) New** in the upper left part of the screen again.
9. The forms for a new email open. Type the following:
    a. To: Write down **Marguerite** and select her email address from the dropdown list
    b. Add a subject: **Second DLP Policy Test**
    c. Add a message or drop a file here: **Hack the IP address 192.168.0.1 and then the IP address 172.16.0.1.**
10. Wait a moment, till the message is saved as a draft.
11. You will see a different policy tip above your message fields. Click on **Show details**.
12. Click on **Override** to be able to send the message anyway.
13. Click **Send** in the lower left part of the screen.
14. Switch to the client system BER-CL01 and login as **Marguerite Ortiz (marguerite@AdatumXXXXXX.onmicrosoft.com)**, with the password **Pa$$w0rd**.
16. Open a new Edge browser window or select the address bar in your browser and go to https://outlook.office365.com.
17. If you are not automatically signed into Microsoft 365 as **Marguerite Ortiz**, then on the Microsoft 365 sign-in page, sign in to **Marguerite's marguerite@AdatumXXXXXX.onmicrosoft.com** account using the password **Pa$$w0rd**.
18. You will see both messages in your inbox.
19. Delete both messages as the last operation in this exercise.

You have now tested your DLP policy successfully.

Exercise 4 – Using Azure Information Protection

Task 1 – Use Azure Information Protection on a client

In this exercise you will use the created AIP label to classify a document and send it via email to **Judy Wyatt** and your personal mail account.

Switch to the client system BER-CL01 and login as **Marguerite Ortiz (marguerite@AdatumXXXXXX.onmicrosoft.com)**, with the password **Pa$$w0rd**.

1. On the client, click at the start symbol, type **Outlook** and open Outlook 2016.
2. On the client, click at the start symbol, type **Word** and open Word 2016.
3. At the first start of Word 2016, you must click on **Accept and start Word**, then select **Office Open XML formats** and click **Ok**.
4. Click on **Blank document**.
5. Write down **Some personally identifiable information (PII).**
6. If the Azure Information Protection bar is visible, click on **PII**. If not, click on **Protect** from the Home Ribbon and select **PII**.
7. In the new window, select the following options:
    a. Select permissions: **Viewer – View Only**
    b. Select users, groups, or organizations: Click on the address book icon and when Outlook opens, select **Judy Wyatt.** Click **To ->** and then **Ok.**
    c. Expire access: Select the next day
8. Click **Apply** to finish the protection process.
9. Click on **File** from the top Ribbon bar.
10. Click on **Save As** on the left menu.
11. Click on OneDrive.
12. Enter **ProtectedDocument** as the name of the file and click **Save** right beside the **Word Document (*.docx)** file type.

Task 2 – Verify AIP policy

You have now created a Word document and protected it with Azure Information Protection by inserting a watermark and encryption. You can now send the document to **Judy Wyatt** and your personal email address, that you have both granted access to the content.

1. Open a new Edge browser window or select the address bar in your browser and go to https://outlook.office365.com.
2. On the Outlook on the web main screen, click on **(+) New** in the upper left part of the screen.
3. The forms for a new email open. Type the following:
    a. To: Write down **Judy** and select her email address from the dropdown list. Then add your personal email address.
    b. Add a subject: **Protected Document Test**

c. Add a message or drop a file here: **Find a protected and restricted document attached to this email.**
d. Click on **Attach** from the top menu and select **Cloud locations**. Select **ProtectedDocuments.docx** from the list and click **Next**.
e. Select **Attach as a copy**.

4. Click **Send** from the upper left part of the screen.

Judy can now work with the file, but when you try to open the file at your personal email account, you can see that you will not be able to view or work with it. Continue with the next exercise.

Exercise 5 – Using Windows Information Protection

Task 1 – Use Windows Information Protection

In this exercise you will test the Windows Information Protection policy from Lab 2, Exercise 2, Task 2 on a client by creating a work document and copy & paste from it to a personal location.

Switch to the client system BER-CL01 and login as **Marguerite Ortiz (marguerite@AdatumXXXXXX.onmicrosoft.com)**, with the password **Pa$$w0rd**.

Perform the following steps:

1. On the client click at the start symbol and open Word 2016.
2. Click on **Blank document**.
3. Write down **Protected business content** into the document.
4. Click on **File** from the top Ribbon bar.
5. Click on **Save As** on the left menu.
6. Click on **Browse** from the menu.
7. Click on the lock symbol left of the file name field and select **Work (AdatumXXXXXX)**.
8. Accept the default name and file path and click **Save**.
9. Back on the Word document, select the written down text, right click on it and select **Copy**.
10. Open a new Edge browser window or select the address bar in your browser and go to https://www.bing.com.
11. Right click into the search field and select **Paste**.
12. A window opens, that tells you: **Can't use work content here.** Click **Ok**.

You have now successfully tested the protection feature that prevents a copy & paste action between a protected Word document and an untrusted website in your Edge browser. Go to the next exercise.

Exercise 6 – Investigate Microsoft 365 Data

Task 1 – Perform a content search for deleted emails

In this exercise, you will use the content search to find emails with the keyword IP address.

Switch to the management system and perform the following steps:

1. Open the Microsoft Edge browser and go to https://protection.microsoft.com.
2. You should still be signed into Microsoft 365 as Ramiro Armenta. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Ramiro's **admin@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. Click on **Permissions** from the left side menu.
4. Click on the **eDiscovery Manager** role.
5. In the **eDiscovery Manager** section, click on **Edit**.
6. The Editing Choose eDiscovery Manager wizard opens. Click on **Choose eDiscovery Manager**.
7. Click on **(+) Add**.
8. Select **Judy Wyatt** from the **Members** list and click **Add**.
9. Click **Done** and then **Save**.

Switch to the client system BER-CL02 and login as **Judy Wyatt (judy@AdatumXXXXXX.onmicrosoft.com)**, with the password **Pa$$w0rd**.

1. Open a new Edge browser window or select the address bar in your browser and go to https://protection.microsoft.com.
2. You should still be signed into Microsoft 365 as Judy Wyatt. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Judy's **judy@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. Open **Search & Investigation** on the left side menu and click on **Content search**.
4. Click on **(+) Guided search** on the top menu.
5. Enter **Content Search Test** into the **Name** field and click **Next**.
6. Select **All locations** and click **Next**.
7. Enter **IP address** into the Keywords box and click **Finish**.

When the content search finishes, you will see all mailbox items that you have created for the sensitive information test of your custom DLP policy. Continue with the next exercise.

Task 2 – Create an eDiscovery case

In this exercise, you will create an eDiscovery case for any violations regarding IP addresses. You will continue using Judy Wyatt's user, who is still in the group of the eDiscovery Managers, that also has the permissions to create an eDiscovery case.

To create an eDiscovery case in the Security & Compliance Center, perform the following steps:

1. Open the Microsoft Edge browser and go to https://protection.microsoft.com.

2. You should still be signed into Microsoft 365 as Judy Wyatt. However, if you have been signed out of Microsoft 365, then on the Microsoft 365 sign-in page, sign in to Judy's **judy@AdatumXXXXXX.onmicrosoft.com** account using a password of **Pa$$w0rd**.
3. Open **Search & Investigation** on the left side menu and click on **eDiscovery**.
4. Click on **(+) Create a case** on the top menu.
5. The New case wizard opens on the right side.
6. Enter **IP Address Violation** into the **Case name** field and click **Save**.
7. Back on the eDiscovery page, click **Open** on your case.
8. On the Core ED page, click on **Hold** from the top menu.
9. Click on **(+) Create** for a new Hold.
10. Enter **IP Address Violation** into the **Name** field and click Next.
11. For the location **Exchange email**, click **Choose users, groups or teams**.
12. Click on **Choose users, groups or teams** again.
13. Enter **Marguerite** into the search field and select **Marguerite Ortiz** from the search results.
14. Click **Choose** and **Done**.
15. Click **Next** in the wizard.
16. Enter **IP address** into the Keywords box and click **Next**.
17. Click **Create this hold** on the Review your settings page.
18. On the Core ED page again, click on **Search** from the top menu.
19. Click on **(+) New search.**
20. Enter **IP Address** into the **Keywords** field and select **Locations on hold** below **Locations**.
21. Click **Save & run**.
22. Enter **IP Address Violation** into the Name field and click **Save**.

You have now created an eDiscovery case with a configured hold and content search.

End of lab