# Lab Answer Key: Module 11: Planning and configuring Rights Management and compliance

# Lab: Configuring Rights Management and compliance

## Exercise 1: Configuring Rights Management in Office 365

#### Task 1: Activate Rights Management in Office 365

1. On LON-CL1, open Microsoft Edge, and then connect to <https://portal.office.com>.
2. Sign in to the Microsoft Office 365 portal as **holly@gsp.Adatumvsxxxx.virsoftlabs.com** with the password ‘Pa55w.rd’.
3. In the app launcher, click the **Admin** icon.
4. In the Office 365 admin center, select **Settings** and then click **Services & add-ins**.
5. Click **Microsoft Azure Information Protection**.
6. On the **Microsoft Azure Information Protection** page, click **Manage Microsoft Azure Information Protection settings**.
7. On the **rights management** page, click **activate**.
8. When prompted with **Do you want to activate Rights Management?**, click **activate.**

#### Task 2: Configure Rights Management for Exchange Online

1. Open the Windows Azure Active Directory Module for Windows PowerShell from the desktop.
2. Type the following commands, and then press Enter after each command to connect to remote Exchange Online with remote PowerShell. Use Holly's credentials to connect.

$Cred = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $Cred -Authentication Basic -AllowRedirection

Import-PSSession $Session

1. Type the following command, and then press Enter to set the IRM sharing location to the region you are in.

Set-IRMConfiguration -RMSOnlineKeySharingLocation "https://sp-rms.eu.aadrm.com/TenantManagement/ServicePartner.svc"

1. Type the following command, and then press Enter to configure Azure Information Protection as a trusted publishing domain.

Import-RMSTrustedPublishingDomain -RMSOnline -name "RMS Online"

1. Type the following command, and then press Enter to set the IRM configuration for licensed users only.

Set-IRMConfiguration -InternalLicensingEnabled $true

1. Type the following command, and then press Enter to test the configuration.

Test-IRMConfiguration -Sender holly@gsp.Adatumvsxxxx.virsoftlabs.com

1. Type the following command, press Enter, and then close Windows PowerShell.

Remove-PSSession $Session

#### Task 3: Configure Rights Management for SharePoint Online

1. In Microsoft Edge, access the Office 365 admin center by using App launcher icon.
2. In the left navigation pane, under **Admin centers**, click **SharePoint**.
3. In the SharePoint admin center, in the left pane, click **settings**.
4. On the **settings** page, in the Information Rights Management (IRM) section, click **Use the IRM service specified in your configuration**, and then click **Refresh IRM Settings**.

#### Task 4: Validate the Azure Rights Management functionality

1. On LON-CL1, open Word 2016.
2. In the Word window, at the top right corner, click **Switch account** or **Sign in**.
3. In the Accounts dialog box, click **Add Account**.
4. In the Sign in dialog box, type **Holly@gsp.Adatumvsxxxx.virsoftlabs.com** , and then click **Next**.
5. Type **Pa55w.rd**, and then click **Sign in**.
6. Close Word 2016.
7. On LON-CL1, open Microsoft Outlook 2016.
8. Create a new email with **Beth Burke** as the recipient.
9. Type a subject, and then type some text in the message body.
10. On the **Options** tab, click **Permission**, and then click **Connect to the Rights Management Server and get templates**. If Windows Security window appears, click **OK** and sign in with Holly's credentials.
11. Click **Permission** again, and then click **Do Not Forward**.
12. Send the message.
13. In Microsoft Edge, connect to **https://gspAdatumvsxxxx.sharepoint.com/sites/marketing**.
14. Click **Documents**, click the **settings** icon, and then click **Library settings**.
15. On the **Settings** page, under Permissions and Management, click **Information Rights Management**.
16. On the **Information Rights Management Settings** page, select the **Restrict permissions on this library on download** checkbox.
17. In the **Create a permission policy title** box, type **Marketing Policy**.
18. In the **Add a permission policy description** box, type **Marketing policy for downloads.**
19. Click **SHOW OPTIONS**.
20. Under Configure document access rights, select the **Allow viewers to write on a copy of the downloaded document** checkbox.
21. Click **OK**.
22. Close Microsoft Edge.
23. Open Microsoft Edge, and then connect to **https://portal.office.com**. Sign in as **Beth@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password **Pa55w.rd**.
24. In the Office 365 portal, in the App launcher, click **Mail**.
25. On the Outlook page, select your time zone and click **Save**.
26. Verify that you received an email from Holly that is IRM protected. Click the message.

You may need to wait for Outlook Web Acess to update with the IRM template. You can also use LON-CL3 to check mail using Outlook 2016.

1. Click the down arrow beside **Reply all**, and then verify that you do not have the option to forward or print the message.
2. In Microsoft Edge, connect to **https://gspAdatumvsxxxx.sharepoint.com/sites/marketing**.
3. Click **Documents**, and then click **document**.
4. After the document opens, try to edit it in Word Online. Verify that you get a message that the document is read-only.
5. Close Microsoft Edge.

**Result**: After completing this exercise, you will have configured Rights Management for Exchange Online and SharePoint Online.

## Exercise 2: Configuring compliance features

#### Task 1: Configure Security & Compliance Center permissions and audit logging

1. On LON-CL1, open Microsoft Edge, and then connect to <https://portal.office.com>.
2. Sign in to the Office 365 portal as **holly@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password ‘Pa55w.rd’.
3. In the app launcher, click the **Admin** icon.
4. In the Office 365 admin center, in the left side menu, select **Admin centers** and then click **Security &Compliance**. If you are connected to the Compliance Center, click **Check out your new Office 365 Security & Compliance Center**.
5. In the Security & Compliance Center, click **Permissions**.
6. Click **Compliance Administrator**, and then click **Edit**.
7. On the **Compliance Administrator** page, under Members, click **Add**.
8. In the Select Members window, click **Beth Burke**, click **add**, and then click **OK**.
9. Click **Save**.
10. Click **To assign permissions for archiving, auditing and retention policies, go to the Exchange admin center**.
11. Click **Compliance Management**, and then click **Edit**.
12. On the **Compliance Management** page, under **Members**, click **Add**.
13. In the Select Members window, click **Beth Burke**, click **add**, and then click **OK**.
14. Click **Save**.
15. Click **Recipient Management**, and then click **Edit**.
16. On the **Recipient Management** page, under **Members**, click **Add**.
17. In the Select Members window, click **Beth Burke**, click **add**, and then click **OK**.
18. Click **Save**.
19. Close the Exchange role groups window.
20. Click **eDiscovery Manager**, and then click **Edit**.
21. On the **eDiscovery Manager** page, under eDiscovery Manager, click **Add**.
22. In the Select Members window, click **Christie Thomas**, click **add**, and then click **OK**.
23. Click **Save**.
24. Click **Search & Investigation**.
25. Click **Audit log search**.
26. On the **Audit log search** page, in the **Activities** drop-down, select **User administration activities**, and then click **Search**.
27. Close Microsoft Edge.

#### Task 2: Configure archive mailboxes

1. On LON-CL1, open Microsoft Edge, and then connect to **https://protection.office.com**.
2. Sign in to the Office 365 portal as **Beth@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password **Pa55w.rd**. Beth is a member of the Compliance Administrator role, so she can connect to the protection website.
3. In the navigation pane, click **Data governance**, and then click **Archive**.
4. In the Archive window, click **Christie Thomas**, and then Ctrl + click **Catherine Richard**.
5. Under Bulk Edit, click **Enable**. In the warning message, click **Yes**, and then click **Close**.
6. Click **Refresh**, and then verify that Christie and Catherine have been enabled for an archive mailbox.
7. Close Microsoft Edge.

#### Task 3: Configure retention tags and policies

1. On LON-CL1, open Microsoft Edge, and then connect to **https://portal.office.com**.
2. Sign in to the Office 365 portal as **holly@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password ‘Pa55w.rd’.
3. In the app launcher, click the **Admin** icon.
4. In the Office 365 admin center, in the left side menu, select **Admin centers** and then click **Exchange**.
5. Under **compliance management**, click **retention tags**.
6. On the **retention Tags** page, click **New tag**, which is the plus sign (**+**), and then select **applied automatically to entire mailbox (default)**.
7. Type **Research User 1 year move to archive** as the name.
8. Select **Move to Archive** as the **Retention action**.
9. Type **365** as the **Retention period**.
10. Click **Save**.
11. On the toolbar, click **New tag**, and then select **applied automatically to entire mailbox (default)**.
12. Type **Default 2 years move to Deleted Items** as the name.
13. Select **Delete and Allow Recovery** as the **Retention action**.
14. Type **730** as the **Retention period**.
15. Click **Save**.
16. On the toolbar, click **New tag**, and then select **applied automatically to a default folder**.
17. Type **Purge Deleted Items 30 days** as the name.
18. Under Apply this tag to the following default folder, select **Deleted Items**.
19. Select **Permanently Delete** as the **Retention action**.
20. Type **30** as the **Retention period**.
21. Click **Save**.
22. On the toolbar, click **New tag**, and then select **applied by users to items and folders (personal)**.
23. Type **2 Year Delete** as the name.
24. Select **Delete and Allow Recovery** as the **Retention action**.
25. Type **730** as the **Retention period**.
26. Click **Save**.
27. On the toolbar, click **New tag**, and then select **applied by users to items and folders (personal)**.
28. Type **Never archive** as the name.
29. Select **Move to Archive** as the **Retention action**.
30. Select **Never** as the **Retention period**.
31. Click **Save**.
32. Click **retention policies**.
33. On the toolbar, click **New**.
34. On the **new retention policy** page, type **Research MRM Policy** as the name.
35. Click **Add** below **Retention tags**.
36. In the select retention tags window, Ctrl+click the following retention tags:

* **Research user 1 year move to archive**
* **Never delete**
* **2 year delete**

1. Click **add**, and then click **ok**. Click **Save**.
2. In the left-hand menu, click **recipients**.
3. On the **mailboxes** page, click **ChristieThomas**, and then click **Edit**.
4. Click **mailbox features** and under **Retention policy** select **Research MRM Policy**, and then click **Save**.
5. Close Microsoft Edge.

#### Task 4: Configure content deletion and preservation policies

1. On LON-CL1, open Microsoft Edge, and then connect to **https://protection.office.com**.
2. Sign in as **holly@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password ‘Pa55w.rd’.
3. Click **Data governance**, and then click **Retention**.
4. Click **Create**.
5. On the **Name your policy** page, enter **Marketing Document Policy** in the **Name** textbox and click **Next**.
6. On the **Settings** page, under **Do you want to retain content?** select **No, just delete content that's older than**, type **7** and verify that **years** is selected.
7. Verify that **when it was created** is selected, and click **Next**.
8. On the **Set your locations page** your locations page select **Let me choose specific locations**.
9. Turn off the option for **Exchange email**.
10. Next to the **SharePoint sites** option click **Choose sites**.
11. On the **Edit locations** page click **Choose sites**.
12. In the search box, enter **https://gspAdatumvsxxxx.sharepoint.com/sites/marketing** and click the **Search** icon.
13. Select the **Marketing** site and click **Choose** and then click **Done**. Click **Next**.
14. On the **Decide if you want to use Preservation Lock** page, click **Next**.
15. On the **Review your settings** page, verify all settings and note any warnings, and then click **Create this policy**.
16. Verify that the **Status** is **On (Pending)**, and then click **Close**.
17. Click **Create**.
18. On the **Name your policy** page, enter **Retain contract details** in the **Name** textbox and click **Next**.
19. On the **Settings** page, under **Do you want to retain content?** select **Yes, I want to retain it**, type **7** and verify that **years** and **when it was created** are selected.
20. Select **Use advanced retention settings**.
21. Verify that **Detect content that contains specific words or phrases** is selected, and click **Next**.
22. In the **Keywords query editor** box, type **Contract** and click **Next**.
23. On the **Choose locations** page, select **Let me choose specific locations**.
24. On the **Choose locations** page, next to **Exchange email**, click **Choose recipients**.
25. On the **Edit locations** page, click **Choose recipients**.
26. Select **Francisco Chaves**, click **Choose**, and then click **Done**.
27. On the **Choose locations** page, next to the **SharePoint sites** option, click **Choose sites**.
28. On the **Edit locations** page, click **Choose sites**.
29. In the search box, enter **https://gspAdatumvsxxxx.sharepoint.com/sites/AcctsProj** and then click the **Search** icon.
30. Select the **Accounts Project** site, click **Choose**, and then click **Done**.
31. On the **Choose locations** page, turn off **OneDrive accounts** and **Office 365 groups**, and then click **Next**.
32. On the **Review your settings** page, verify all settings and note any warnings, and then click **Create this policy**.
33. Verify that the **Status** is **On (Pending)**, and then click **Close**.
34. Close Microsoft Edge.

#### Task 5: Configure data loss protection policies

1. Open Microsoft Edge, and then connect to **https://protection.office.com**.
2. Sign in to the Office 365 portal as **Beth@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password **Pa55w.rd**.
3. In the navigation pane, click **Data loss prevention** and then click **Policy**.
4. Click **Create a policy**.
5. On the **Start with a template or create a custom policy** page, verify that **Custom** is selected, and then click **Next**.
6. On the **Name your policy** page, type **Test DLP** in Name textbox, and then click **Next**.
7. On the **Choose locations** page, select **All locations in Office 365** and click **Next**.
8. On the **Customize the types of content you want to protect** page, select **Use advanced settings**, and click **Next**.
9. On the **Customize the types of content you want to protect** page, click **New rule**.
10. On the **Create a new rule** page, in the **Name** field, type **Scan for IP address**.
11. Under **Content contains**, click the **Add** drop-down and then select **Sensitive info types**.
12. In **Sensitive info types** window, click **Add**. Scroll down in the list and select **IP Address**, click **Add**, and then click **Done**.
13. Click the **Add a condition** drop-down, and select **Content is shared**.
14. Under **Content is shared**, select **with people outside my organization**.
15. Under **Actions**, click **Add an action**, and then select **Restrict access to the content**.
16. Under **User notifications**, enable the option to **Use notifications to inform your users and help educate them on the proper use of sensitive information.**
17. Under **Incident reports**, enable the option to **Use email incident reports to notify you when a policy match occurs.**
18. Under **User overrides**, enable the option to **Let people who see the tip override the policy and share the content.** Note the additional options, and then click **Save**.
19. On the **Customize the types of content you want to protect** page, click **Next**.
20. On the **Do you want to turn on the policy or test things out first?** page, select **Yes, turn it on right away** and then click **Next**.
21. On the **Review your settings** page, verify your settings, and then click **Create**.
22. On the **Test DLP\* page, verify that the** Status\*\* is **On**, and then click **Close**
23. Close Microsoft Edge.

#### Task 6: Create compliance check content

1. Open Microsoft Edge, and then connect to **https://portal.office.com**.
2. Sign in to the Office 365 portal as **Beth@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password **Pa55w.rd**.
3. On the Office 365 home page, click **Mail**.
4. Click **New**, type the new Microsoft account email address that you created for this course in the **To** line, type **Server IP address** as the **Subject**, type **My IP is 192.168.1.15** as the message body, and then wait for a minute or two until the policy tip appears at the top of message.
5. At the top of the message, click **Show details**.
6. Click **Override**, and then click **Send**.
7. Close Microsoft Edge.

#### Task 7: Validate the configuration

1. Open Microsoft Edge, and then connect to **https://outlook.com**. Sign in with your Microsoft account.
2. Click the message from Beth Burke with the subject **Server IP address**.
3. Close Microsoft Edge.
4. Open Microsoft Edge, and then connect to https://portal.office.com.
5. Sign in to the Office 365 portal as **Christie@gsp.Adatumvsxxxx.virsoftlabs.com** with the password **Pa55w.rd**.
6. Click **Mail**.
7. Select your time zone, and then click **Save**.
8. In the left pane of Christie's mailbox, under Folders, click **More**.
9. Verify that a folder named **In-Place Archive - Christie Thomas** has been created.
10. Close Microsoft Edge.
11. Open Microsoft Edge, and then connect to https://portal.office.com.
12. Sign in to the Office 365 portal as **Beth@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password **Pa55w.rd**.
13. Click **Mail**.
14. Verify that you have received notification about message you sent to your personal account. This message should have **Rule detected** words in the subject.

**Result**: After completing this exercise, you will have implemented the Office 365 compliance features.

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.