Exercise 1 – Implementing DLP

Objective:

Practice creating, customizing, and reviewing DLP policies using both the Exchange Admin Center and PowerShell.

Tasks:

Using the Exchange Admin Center

1. Create a new **DLP policy** based on the following:
   - Name: **Confidential Info - Canada**
   - Template: **Canada Personally Identifiable Information (PII)**
   - Enforcement Mode: **Test with Policy Tips**
2. Modify the policy to:
   - Add a new custom rule that **warns** the sender if the message includes sensitive information.
   - Apply the rule to emails sent **outside** the organization.
3. Create another DLP policy from scratch **(without using a template):**
   - Name: **Custom Credit Card Filter**
   - Add a rule that:
     - Detects credit card numbers
     - Blocks the message if found
     - Allow the sender to override with justification
4. Review all DLP policies and analyze the rules created.

Using the PowerShell Exchange Management Shell (EMS)

1. List all available DLP policy templates.
2. Create a DLP policy:
   - Name: **Finance DLP Block**
   - Template: **Canada Financial Data**
   - Enforcement Mode: **Enforce**

3. Create a transport rule linked to the **Finance DLP Block policy** that:
    - Notify the sender when the content includes a credit card number.
    - Applies only to external recipients.
4. List all DLP policies currently deployed in the organization.

Exercise 2 – Implementing Anti-Malware Policies

Objective:

Explore the creation and customization of **anti-malware policies using EAC and PowerShell.**

Tasks:

Using the Exchange Admin Center:

1. Review the default anti-malware policy under Protection > Malware Filter.
2. Create a new policy with:
    - Name: **Attachment Blocker**
    - Action: **Delete the message and notify the sender**
    - Condition: Applies to messages sent to an external domain (e.g., @domainXX.com)
3. Create another policy named **Warn Internal Users** that:
    - Deletes only the infected attachment.
    - Send a notification to the administrator.
4. Verify all created anti-malware policies and their associated settings.

Using the Exchange Management Shell (EMS):

1. List all existing anti-malware policies.
2. Review the notification settings applied to a selected anti-malware policy.
3. Force a malware definition update using the appropriate script.