W-4, D-2

1. How to create alert policies? What are those policies used for?

Alert Policy	✓ Use alert policies to **track user and admin activities**, malware threats, or data loss preventions, mail flow activities, permissions in your organization. ✓ After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications.
How Alert Policy Works	
Please go to – https://protection.office.com Please navigate to – **Alerts > Alert policies** ✓ **Name your Alert** Type the Name, Choose **Severity** & **Category**	
✓ **Create alert settings** Choose **activity is** and **Add condition** if required	
✓ **Set your recipients** Type **send email notification** and set **Daily notification limit**	
✓ **Review your settings**	

2. Assigning permission in SCC.

Please go to – https://protection.office.com Please navigate to – **Permissions** You will see a list of default permissions available. Click any one & scroll down. Click **Edit** under **Member** section
Click **Choose members** & add a member for this role.

W-4, D-2

3. How to import .PST files?

Roles required	✓ You have to be assigned the **Mailbox Import Export role, Mail Recipients role** in Exchange Online. By default, this role is assigned to the **Organization Management** and **Recipient Management** roles groups. Or, ✓ You have to be a global administrator in your organization.
✓ Step 1: **Copy the SAS URL and install AzCopy** o This URL is a combination of the **network URL** for the **Azure Storage location** in the Microsoft cloud for your organization and a **Shared Access Signature (SAS)** key. o This key provides you with the necessary permissions to upload PST files to your Azure Storage location. o Need to download **Azure AzCopy** ✓ Step 2: **Upload your PST files to Microsoft 365** ✓ (Optional) Step 3: **View a list of the PST files uploaded** ✓ Step 4: **Create the PST Import mapping file** ✓ Step 5: **Create a PST Import job** ✓ Step 6: **Filter data and start the PST Import job**	
✓ You have to perform **Step 1 only once** to import PST files to Microsoft 365 mailboxes. ✓ Upload PST file must be less than 20 GB	

4. What is Submission explorer? How to submit emails?

Submission Explorer	✓ In Microsoft 365 organizations with mailboxes in Exchange Online, admins can use the Submissions portal in the Security & Compliance Center to submit email messages, URLs, and attachments to Microsoft for scanning. ✓ When you submit an email, you will get information about any policies that may have allowed the incoming email into your tenant, as well as examination of any URLs and attachments in the mail.
Roles Required	✓ **Organization Management** or **Security Administrator** in the **Security & Compliance Center** ✓ **Organization Management** or **Hygiene Management** in **Exchange Online**

W-4, D-2

Submit Emails through Submission Explorer
Please go to – https://protection.office.com Please navigate to – ① **Threat management** > ② **Submission** > ③ **New Submission** For **Email** – Choose **Object type, Submission format, Reason for submission** & press **submit** For **URL/Attachment** – Mention URL link/download the attachment, choose **Reason for submission** & press **submit**

5. What are the reasons for a user to be restricted from sending email? How to unblock users from restricted users?

Reasons for Restriction from Sending Email	✓ If a user exceeds one of the outbound sending limits (e.g. 30 messages/minute) as specified in the service limits or in outbound spam policies. ✓ The user is restricted from sending email, but they can still receive email. ✓ When they try to send email, the message is returned in a **non-delivery report (NDR)** with the error code **5.1.8 (Access Denied)** and the following text:

Unblock user from Restricted User
✓ In the Security & Compliance Center, go to **Threat management** > **Review** > **Restricted users** ✓ Find and select the user that you want to unblock. In the **Actions** column, click **Unblock**. ✓ Click **Next** when done. ✓ The next screen has recommendations to help prevent future compromise. Enabling multi-factor authentication (MFA) and changing the passwords are a good defense. Click Unblock user when done. ✓ It may take 30 minutes or more before restrictions are removed.

How to Resolve the Issue (5.1.8 – Access Denied)
✓ If the user is doing is willingly, admin may warn user and unblock. ✓ If the user account is hacked, then admin can **reset password, enable MFA, Do MHA, try Message trace**

W-4, D-2

6. What is the purpose of Anti-Phishing & Anti-Spam Policies? How to set up these policies?

Purpose of Anti-Phishing & Anti-Spam Policies	✓ In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, email messages are automatically protected against spam and malware by EOP. ✓ Spam is unsolicited and unwanted email. Malware is viruses and spyware. ✓ Viruses infect other programs and data, and they spread throughout your computer looking for programs to infect. ✓ Spyware is a specific type of malware that gathers your personal information (for example, sign-in information and personal data) and sends it back to the malware author. ✓ EOP has built-in inbound and outbound malware filtering to help protect your organization from malicious software, and built-in spam filtering to help protect your organization from both receiving and sending spam (for example, in case of compromised accounts). ✓ Admins don't need to set up or maintain the filtering technologies because they're enabled by default. However, you can customize the settings based on the needs of your organization.
Anti-phishing	✓ In the **Security & Compliance Center**, choose **Threat management** > **Policy** > **ATP anti-phishing**. ✓ Click **Default policy**. ✓ In the **Impersonation** section, click **Edit**, and then specify the following settings: o On the **Add users to protect** tab, turn protection on. o On the **Add domains to protect** tab, turn on **Automatically include the domains I own**. If you have custom domains, add those as well. o On the **Actions** tab, select **Quarantine the message** for both the **impersonated user** and **impersonated domain** options. In addition, turn on impersonation safety tips. o On the **Mailbox intelligence** tab, make sure mailbox intelligence is turned on. In addition, turn on mailbox intelligence-based impersonation protection. In the **If email is sent by an impersonated user** list, choose **Quarantine the message**. o On the **Add trusted senders and domains** tab, specify any trusted senders or domains that you want to add. o On the **Review your settings** tab, after you have reviewed your settings, click **Save**. ✓ In the **Spoof** section, click **Edit**, and then specify the following settings: o On the **Spoofing filter settings** tab, make sure anti-spoofing protection is turned on.

	○ On the **Actions** tab, choose **Quarantine the message**. ○ On the **Review your settings** tab, after you have reviewed your settings, click **Save**. (If you didn't make any changes, click **Cancel**.) ✓ Close the default policy settings page.
Anti-Spam Protection	Anti-spam protection is available in subscriptions that include EOP. 1. In the Security & Compliance Center, choose **Threat management** > **Policy** > **Anti-spam**. 2. On the **Custom** tab, turn **Custom settings** on. 3. Expand **Default spam filter policy**, click **Edit policy**, and then specify the following settings: ○ In the **Spam and bulk actions** section, set the threshold to a value of 5 or 6. ○ In the **Allow lists** section, review (and if necessary, edit) your allowed senders and domains. 4. Click **Save**.

7. How to create an outbound spam policy?

Please go to – https://protection.office.com Please navigate to – **Threat management > Policy > Anti-spam settings > Create an outbound policy >** type a suitable name
Check **notification** if required.
Set **Recipient Limits** for hourly & daily limit (0 to max 10000)
Set **Automatic Forwarding**
Set **Applied to** > **Add Condition >** press **Save**