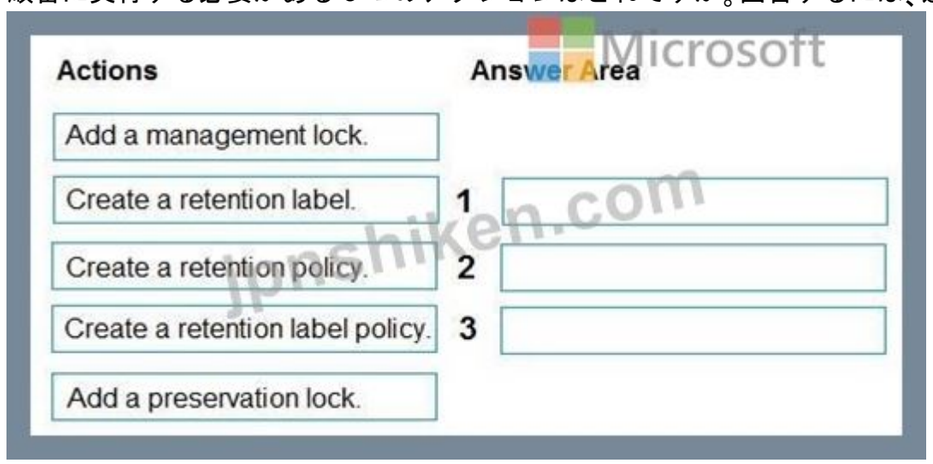
Microsoft.SC-401J.v2026-10-01.q113

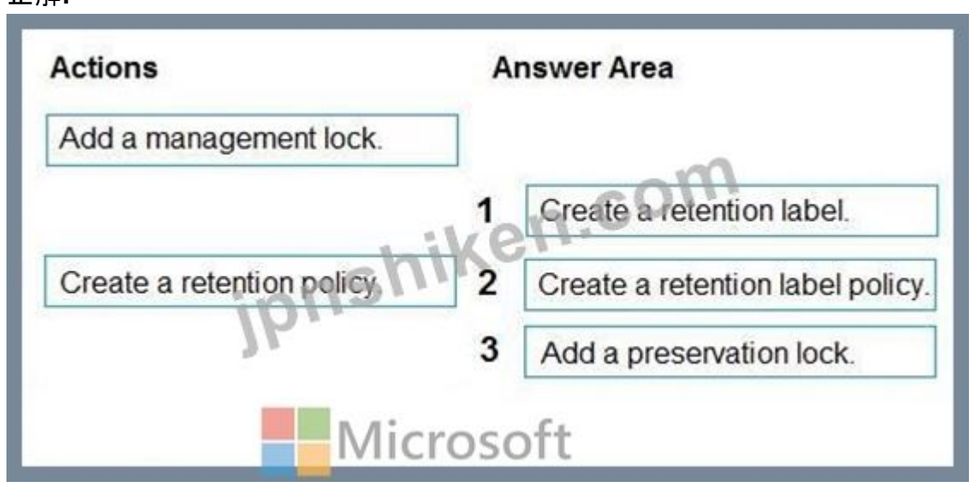
試験コード：	SC-401J
試験名称：	Administering Information Security in Microsoft 365 (SC-401日本語版)
認証ベンダー：	Microsoft
無料問題の数：	113
バージョン：	v2026-10-01
ページの閲覧量：	102
問題集の閲覧量：	1136

https://www.jpnshiken.com/shiken/Microsoft.SC-401J.v2026-10-01.q113.html

質問: **1**
ドラッグアンドドロップの質問
Microsoft 365 テナントがあります。
新しい規制要件では、特許IDを含むすべての文書にラベルを付け、10年間保管した後、削除することが定められています。保管設定を適用するために使用するポリシーは、いかなる者によっても無効化または削除されてはなりません。
規制要件を実装する必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock

質問: **2**
Microsoft 365 E5 サブスクリプションをお持ちです。
クレジットカード番号を含むメッセージや文書は、作成後12ヶ月で自動的に削除されるようにする必要があります。管理作業を最小限に抑えるソリューションが必要です。
どの 2 つのコンポーネントを作成する必要がありますか? それぞれの正解はソリューションの一部を示します。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. 機密ラベルの自動ラベル付けポリシー
B. 機密ラベル
C. 保持ラベルの自動ラベル付けポリシー
D. 保持ラベル
E. 機密情報タイプ (SIT)
正解: **(**正解を表示します**)**
1. Create a retention label that retains and delete contents after 12 months
2. Create an Auto Labeling policy "Auto Apply Label" for a retention label

質問: **3**
Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションがあります。
ユーザーがサードパーティのクラウド ストレージ サービスにドキュメントをアップロードしたときにアラートを受信するようにする必要があります。
何を使うべきでしょうか?
A. インサイダーリスクポリシー
B. ファイルポリシー
C. 機密ラベル
D. アクティビティポリシー
正解: **B (**コメントを発表する**)**
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies
https://learn.microsoft.com/en-us/defender-cloud-apps/policies-information-protection

質問: **4**
Microsoft 365 サブスクリプションをお持ちです。
次の表に示す Microsoft Purview 監査ソリューションを使用するかどうかを評価しています。

Name	Description
Solution1	Control auditing by using audit log retention policies.
Solution2	Export audit records to a CSV file.
Solution3	Retain audit logs for one year.

Microsoft Purview Audit (Standard) を実装する予定です。

どのようなソリューションを使用できますか?
A. ソリューション2とソリューション3のみ
B. ソリューション2のみ
C. ソリューション3のみ
D. ソリューション1とソリューション2のみ
E. ソリューション1、ソリューション2、ソリューション3
正解: **B** (コメントを発表する)

質問: **5**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com" を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク6
ブラウザーによる fabrikam.com へのファイルのアップロードを制限するエンドポイント データ損失防止 (エンドポイント DLP) ポリシーを作成する予定です。
fabrikam.com がエンドポイント DLP ポリシーによって制限されるように、エンドポイント DLP 設定を構成する必要があります。
現時点ではエンドポイント DLP ポリシーを作成する必要はありません。
正解:
To configure an Endpoint DLP policy that restricts browser uploads to a specific domain, first create a "Sensitive service domain group" with the domain you want to block. Then, create a new DLP policy [not needed], select "Devices" as the location, and in the rule's action, choose "Upload to a restricted cloud service domain" and select "Block.". Finally, in the rule's conditions, select the "Content contains" activity and add sensitive labels or other conditions as needed.
Create a sensitive service domain group
Step 1: Go to the Microsoft Purview portal and navigate to Data loss prevention > Settings (gear icon).
Step 2: Select Sensitive service domain groups and click Create sensitive service domain group.
Step 3: Give the group a name (e.g., "Restricted Upload Domains").
Step 4: Enter the specific domain you want to block in the "Sensitive service domain" field. [Enter fabrikam.com] You can use wildcards for subdomains (e.g., *.contoso.com) and can add multiple domains to the group.
Step 5: Select Save.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-configure-endpoint-settings

質問: **6**

次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Description
User1	• User 1 is a regional manager. • User1 is assigned the Reader role. • Three department managers report to User1.
User2	• User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	• User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	• User4 is the assistant of User1. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User1.

jpnshiken.com Microsoft

Microsoft Purview インサイダー リスク管理では、どのユーザーが潜在的に影響の大きいユーザーとしてフラグ付けされますか?

A. ユーザー1、ユーザー2、ユーザー3、ユーザー4
B. ユーザー1、ユーザー2、ユーザー3のみ
C. ユーザー2とユーザー3のみ
D. ユーザー1とユーザー2のみ
正解: **(**正解を表示します**)**

質問: **7**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Teams の保持ポリシーを実装する予定です。
保持できるアイテムの種類はどれですか?
A. 埋め込み画像
B. Teams モバイル クライアントからの音声メモ
C. コードスニペット
正解: **(**正解を表示します**)**
Microsoft Teams, What's included for retention and deletion
Teams chats messages, channel messages, and private channel messages can be deleted by using retention policies for Teams, and in addition to the text in the messages, the following items can be retained for compliance reasons: Video clips, *embedded images*, tables, hypertext links, links to other Teams messages and files, and card content.
Reference:
https://learn.microsoft.com/en-us/purview/retention-policies-teams

質問: **8**

注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
最近、会社の開発者が Azure ストレージ アカウント キーをプレーン テキストで第三者に電子メールで送信していることが分かりました。
Azure ストレージ アカウント キーを電子メールで送信する場合は、電子メールが暗号化されていることを確認する必要があります。
解決策: 機密情報の種類に一致するメール フロー ルールを構成します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解**: (**正解を表示します**)**
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
Mail flow rules (transport rules) can detect sensitive info, but they are limited in encryption capabilities.
DLP policies provide more advanced protection and integration with Microsoft Purview for sensitive info detection.

質問**: 9**
ホットスポットに関する質問
Site1 という名前の Microsoft SharePoint Online サイトと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Member of
User1	Members group of Site1
User2	Owners group to Site1
Admin1	SharePoint Administrator role

次の図に示すように、DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

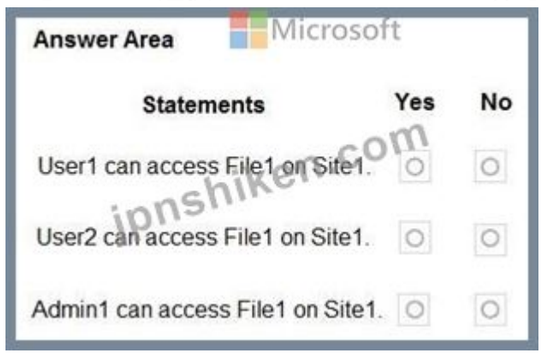


DLP1をサイト1に適用します

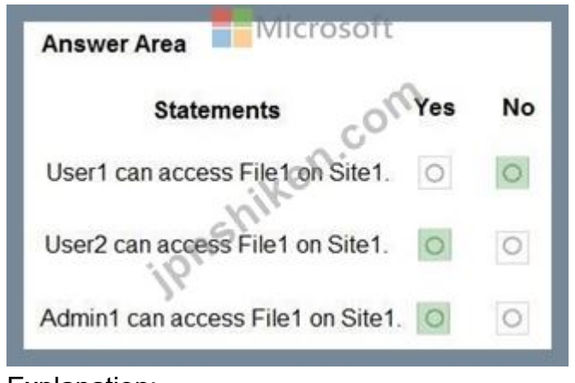
ユーザー1がサイト1にファイル1というファイルをアップロードします。ファイルはDLP1ルールのいずれにも一致しません。ユーザー2はファイル1を更新し、DLP1ルールに一致するデータを追加します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

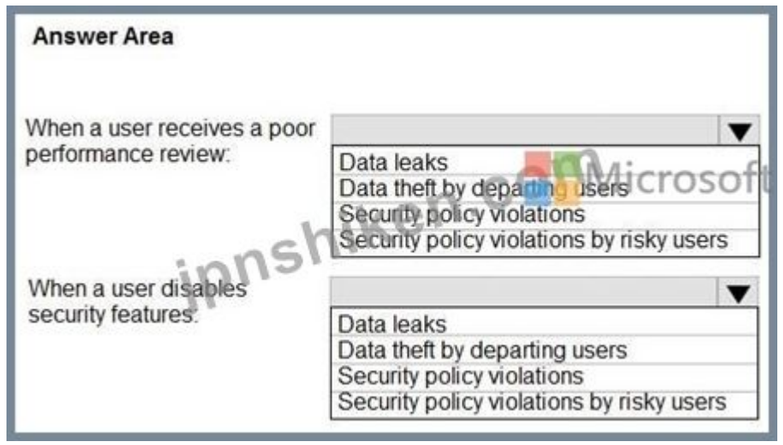


正解:



Explanation:
Box 1: No
Note: Actions
Any item that makes it through the conditions filter will have any actions that are defined in the rule applied to it. You'll have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action you need to choose from these options:
Box 2: Yes
User2 is the last modifier of the file.
Box 3: Yes
Users assigned the SharePoint Administrator role have access to the SharePoint admin center and can create and manage sites (previously called "site collections"), designate site admins, manage sharing settings, and more.
Reference:
https://learn.microsoft.com/en-us/sharepoint/sharepoint-admin-role

質問**: 10**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を実装する予定です。
次の要件を満たすポリシー テンプレートを推奨する必要があります。
- ユーザーが低評価を受けた場合のリスク指標とスコアリングを含む
業績レビュー。
- ユーザーがデバイスのセキュリティ機能を無効にした場合のリスク指標とスコアが含まれます。
各要件にはどのテンプレートを使用する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。注: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Box 1: Security policy violations by risky users

Contain risk indicators and scoring for when a user receives a poor performance review.

Security policy violations by risky users

Users that experience employment stressors might be at a higher risk for inadvertent or malicious security policy violations. These stressors could include a user being placed on a performance improvement plan, having a poor performance review, or experiencing a demotion. This policy template starts risk scoring based on these indicators and activities associated with these types of events.

Box 2: Security policy violations

Contain risk indicators and scoring for when a user disables security features on a device.

Security policy violations

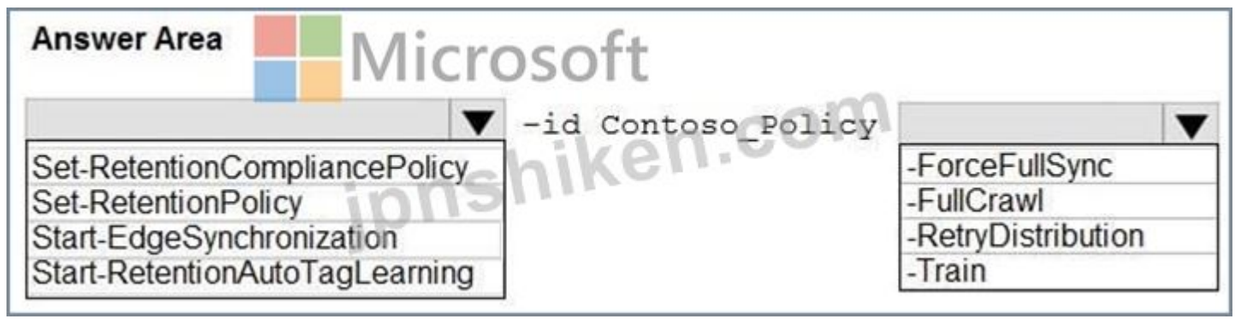
In many organizations, users have permission to install software on their devices or to modify device settings to help with their tasks. Either inadvertently or with malicious intent, users might install malware or *disable important security features* that help protect information on their device or on your network resources. This policy template uses security alerts from Microsoft Defender for Endpoint to start scoring these activities and focus detection and alerts to this risk area. Use this template to provide insights for security policy violations in scenarios when users might have a history of security policy violations that might be an indicator of insider risk.

Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-policy-templates

質問: **11**
100 人のユーザーと Group1 という名前の Microsoft 365 グループを含む Microsoft 365 サブスクリプションがあります。
すべてのユーザーは Windows 11 デバイスを所有しており、Microsoft SharePoint Online と Exchange Online を使用しています。
Label1 という名前の機密ラベルが、Group1 の既定のラベルとして公開されます。
Sublabel1 と Sublabel2 という名前の 2 つのサブラベルを Label1 に追加します。
Sublabel1 の設定が Group1 にデフォルトで適用されていることを確認する必要があります。
何をすべきでしょうか?
A. Label1 のポリシーを変更します。
B. Sublabel1 のすべての設定を Label1 に複製します。
C. Label1 のポリシーを削除し、Sublabel1 を公開します。
D. サブラベル1の順序を変更します。
正解: **(正解を表示します)**
To ensure a sublabel is applied by default to a Microsoft 365 group when the parent label is the default, you must publish the desired sublabel and set it as the default for the group in the Microsoft Purview compliance portal, rather than trying to manipulate the parent label's policy.
The original parent label should not be set as the default for the group anymore, as sublabels override the parent's default status.
Reference:
https://learn.microsoft.com/en-us/purview/sensitivity-labels

質問: **12**
ホットスポットに関する質問
次のラベルを含む Contoso Policy という名前の保持ラベル ポリシーを作成します。
10年後に削除
5年後に削除
保持しない
Contoso_Policy は、Microsoft SharePoint Online サイトのコンテンツに適用されます。
数日後、ラベル ポリシーの [プロパティ] ページに次のメッセージが表示されます。
- ステータス: オフ (エラー)
- ポリシーの展開に予想よりも時間がかかっています
ポリシーを再開する必要があります。
コマンドをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

https://docs.microsoft.com/en-us/powershell/module/exchange/set-retentioncompliancepolicy

質問: 13

User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Microsoft Purview インサイダー リスク管理を展開します。

User1 に関連するインサイダー リスク管理イベントが特定のユーザーのみに表示されるようにする必要があります。

何を創造すべきでしょうか?

A. 検出グループ

B. グローバル除外

C. インジケーターのバリアント

D. 優先ユーザーグループ

正解: **D (**コメントを発表する**)**

To restrict management of Microsoft Purview Insider Risk Management events to specific users, you can utilize Priority User Groups and Administrative Units. Priority User Groups allow you to designate which users can view data related to specific users in Insider Risk Management, while Administrative Units enable you to scope user permissions to geographical areas or departments.

Priority User Groups (PUGs):

Purpose:

PUGs allow you to create groups of users who are deemed high-risk and designate which users (e.g., investigators, analysts) can view data related to those high-risk users.

How to use:

Create a PUG in the Insider Risk Management settings.

When creating the PUG, you'll designate which users (or Insider Risk Management role groups) can view data related to the users within that PUG.

This ensures that only authorized personnel can access and manage alerts and cases associated with those high-risk users.

Reference:

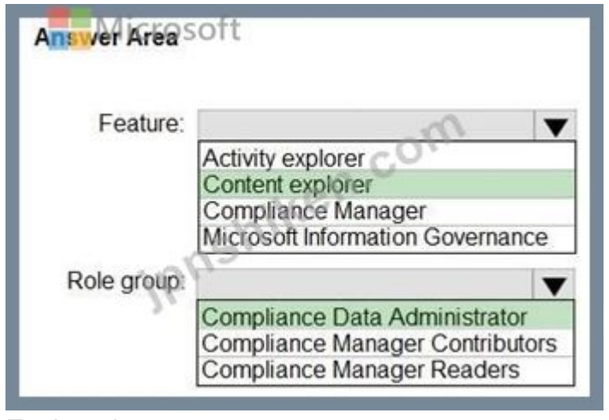
https://learn.microsoft.com/en-us/purview/insider-risk-management-users

質問: **14**
ホットスポットに関する質問
Classifier1 という名前のトレーニング可能な分類子を含む Microsoft 365 E5 テナントがあります。
Classifier1の精度を高める必要があります。解決策としては、最小権限の原則を適用する必要があります。
どの機能を使用する必要がありますか? また、どのロール グループに追加する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:



Explanation:
Box 1: Content Explorer
Increase classifier accuracy
Classifiers, like sensitive information types (SIT) and trainable classifiers are used in various kinds of policies to identify sensitive information. Like most such models, sometimes they identify an item as being sensitive that isn't. Or, they may not identify an item as being sensitive when it actually is. These are called false positives and false negatives.
Box 2: Compliance data administrator
Permissions
In order to get access to the content explorer tab, an account must be assigned membership in any one of these roles or role groups.
Microsoft 365 role groups
Global administrator
Compliance administrator
Security administrator

*-> Compliance data administrator
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-increase-accuracy
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

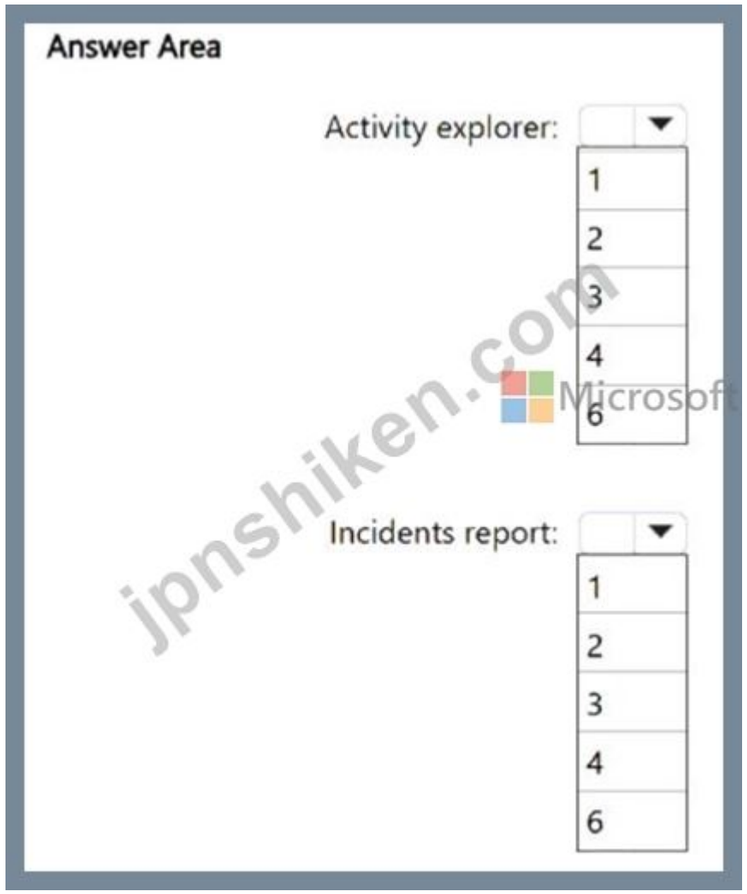
質問: **15**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションがあり、そこには Site1 という名前の Microsoft SharePoint Online サイトが含まれています。Site1 には、File1、File2、File3 という名前の 3 つのファイルが含まれています。
次の表に示すデータ損失防止 (DLP) ポリシーを作成します。

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

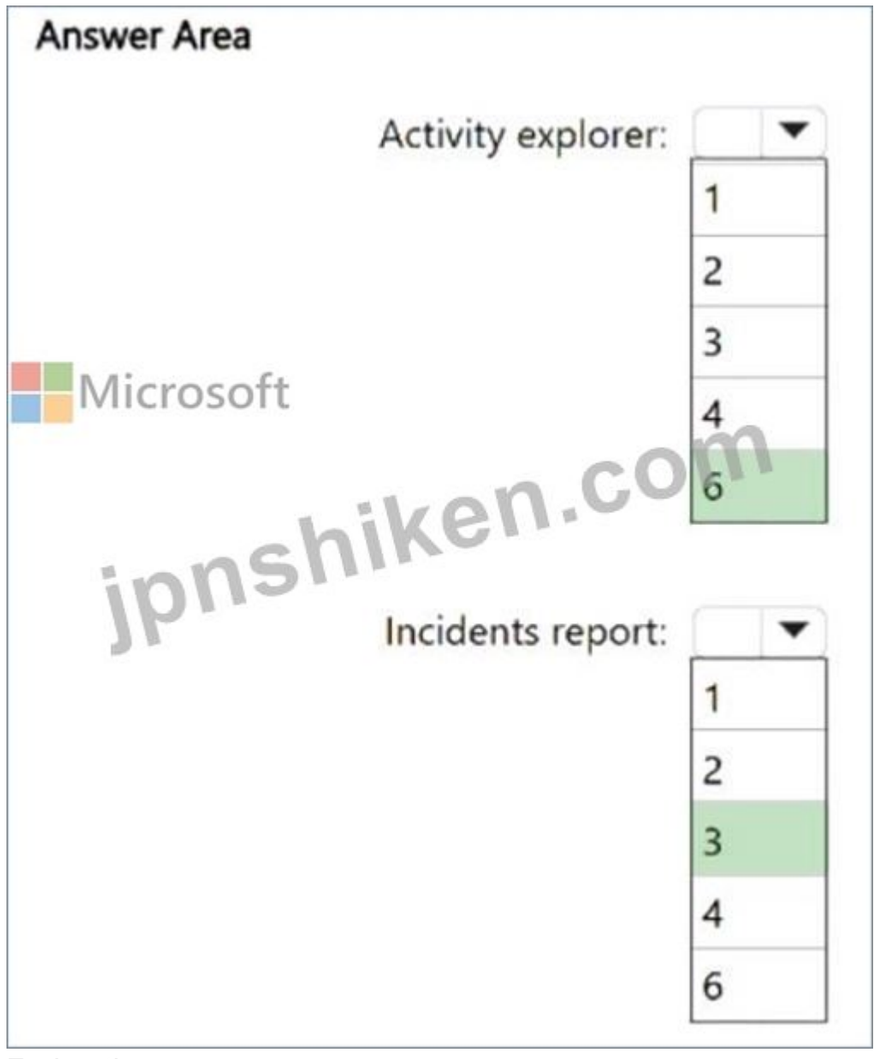
各ファイルに一致する DLP ルールを次の表に示します。

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

アクティビティ エクスプローラーに追加される DLP ポリシー一致イベントの数はいくつですか。また、DLP インシデント レポートに追加されるポリシー一致の数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。


Answer Area
Activity explorer:
1
2
3
4
6
Incidents report:
1
2
3
4
6

正解:



Microsoft
jpnshiken.com

Explanation:

A "DLP policy matches event" is when a user's activity, such as sharing a file or sending an email, triggers a predefined set of rules in a Data Loss Prevention (DLP) policy. When a match occurs, the DLP system can then take a configured action, such as alerting administrators, notifying the user, or restricting access to the data. This event signifies a potential policy violation, such as sensitive information being sent externally or moved to an unauthorized location.

Box 1: 6

The Activity explorer displays DLP policy matches as detailed events sourced from audit logs, providing a historical view of user activities and their impact on sensitive information. It allows users to filter events by various criteria like date, user, activity type, and location to monitor the effectiveness of DLP policies. Events in the Activity explorer can represent partial matches (where only some conditions were met) and full matches, with details on the conditions that triggered the match available through further filtering or by reviewing alert details in the DLP alerts interface.

* File1

Rule11 and Rule12 are both in DLP1.

2 events.

Note:

When an item matches multiple DLP rules, DLP goes uses through a complex algorithm to decide which actions to apply. Endpoint DLP applies the aggregate or sum of most restrictive actions.

DLP uses these factors when making the calculation.
* File2
Rule21 and Rule22 are both in DLP2.
2 events.
* File3
Rule11 is DLP1, and Rule22 is in DLP2.
2 events.
Box 2: 3
The Incidents report displays DLP policy matches by aggregating them to an item-level view, meaning a single email that matches multiple rules will only show up once in this report. This contrasts with the Policy Matches report, which counts each rule match separately. The Incidents report is better for identifying specific problematic content, while the Policy Matches report is better for fine-tuning individual rules.
There are 3 files items, so there will be 3 matches.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
https://learn.microsoft.com/en-us/purview/data-classification-activity-explorer

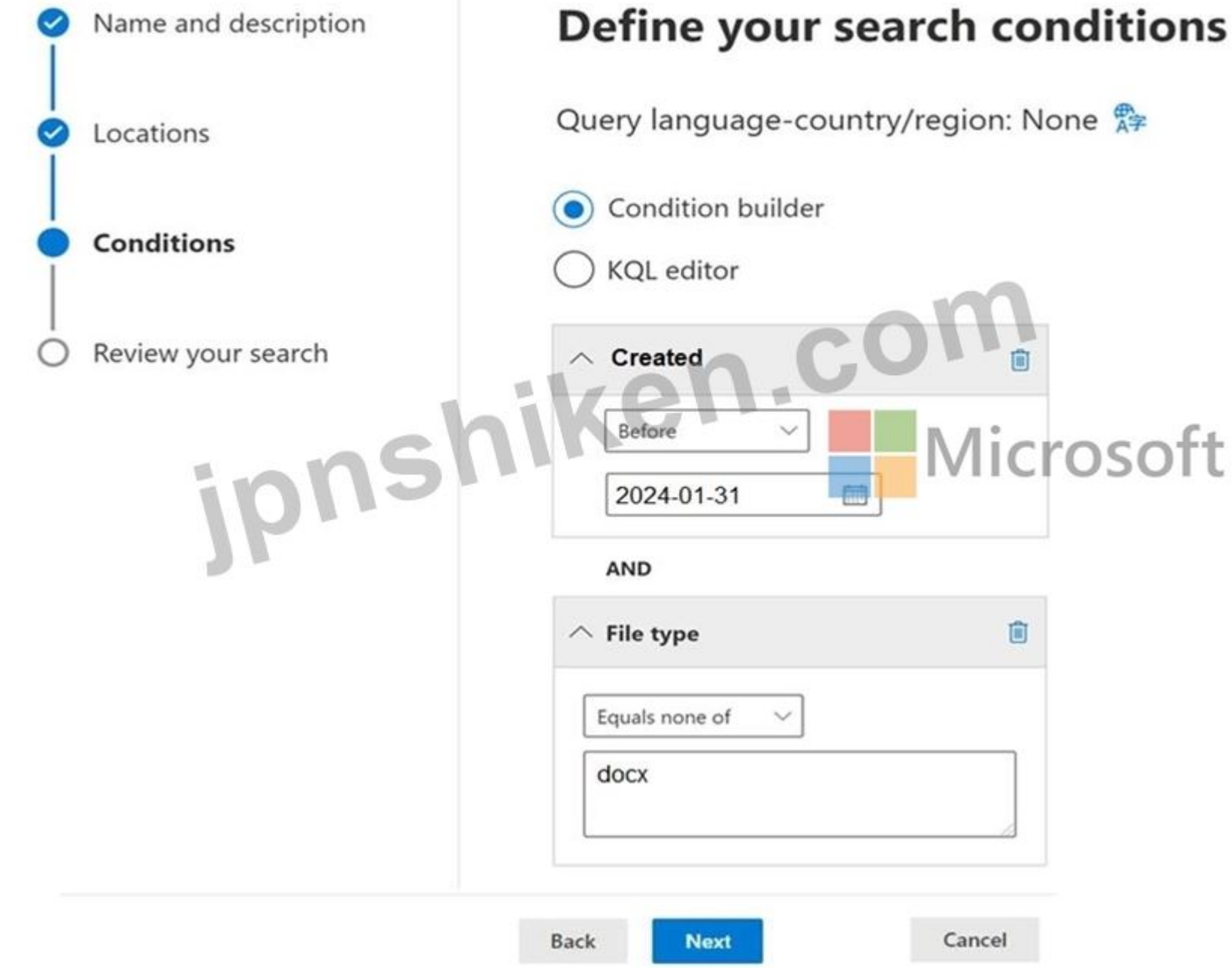
質問: 16
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
すべてのユーザーに Microsoft 365 Copilot ライセンスが割り当てられます。
Microsoft Purview Data Security Posture Management for AI (DSPM for AI) を展開します。
ユーザー1がAIインタラクションイベントのプロンプトと応答を分析できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 をどの 2 つのロール グループに追加する必要がありますか? それぞれの正解はソリューションの一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. セキュリティリーダー
B. コンテンツエクスプローラーリストビューアー
C. インサイダーリスク管理調査員
D. 情報保護アナリスト
E. コンテンツエクスプローラー コンテンツビューアー
正解: (正解を表示します)
Content Explorer Content Viewer
Allows a user to view the full content of items surfaced by Purview (including AI interactions).
■
Required for analyzing actual prompts and responses, not just metadata.
■
More privileged than List Viewer, which only shows counts.
■
Information Protection Analysts
Allows the user to investigate data-classification and data-protection insights, including AI-
■
related data security issues.
Provides Purview-level analysis capabilities without broad security permissions.
■

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
ホットスポットに関する質問
Microsoft 365 サブスクリプションをお持ちです。
Site1 という名前の Microsoft SharePoint Online サイトがあります。Site1 には、次の表に示すファイルを含むドキュメント ライブラリがあります。

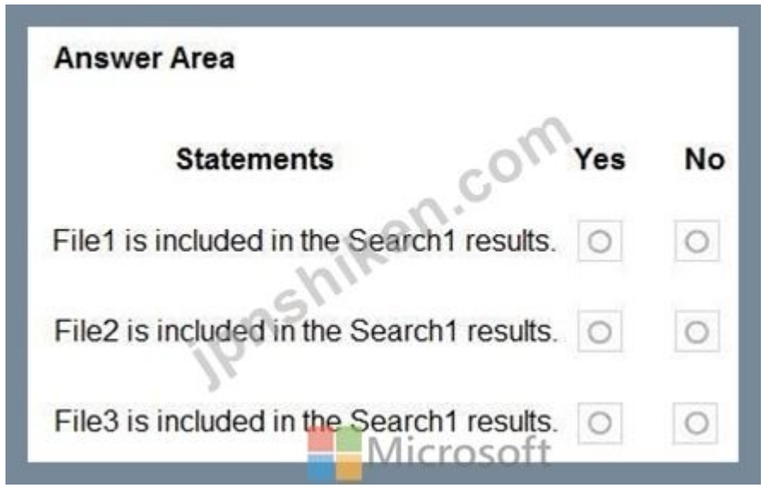
Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

Microsoft Purview コンプライアンス ポータルから、Site1 に対して、次の図に示すように、日付が YYYY-MM-DD 形式の Search1 という名前のコンテンツ検索を作成します。



jpnshiken.com
Microsoft

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:
Box 1: No
File1 has the file type DOCX.
Search1 has File Type Equals none of docx.
File1 is not included in Search1.
Box 2: No
File2 is created on February 5, 2024.
Search1 has the condition for a file to be created before January 1, 2024.
File2 is not included in Search1.
Box 3: Yes
File3 has file type PNG, which does not equal docx.
File3 is created on May 4, 2023, which is before January 1, 2024.
File3 is included in Search1.

質問: 18
次の表に示すアダプティブ スコープを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type	Query
Scope1	Users	`FirstName starts with User`
Scope2	SharePoint Online sites	`SiteTitle starts with Site`

次の表に示す保持ポリシーを作成します。

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

どの保持ポリシーが保存ロックをサポートしていますか?

A. RPolicy2のみ

B. RPolicy3のみ

C. RPolicy1 と RPolicy2 のみ

D. RPolicy1 と RPolicy3 のみ

E. RPolicy1、RPolicy2、およびRPolicy3

正解: **(正解を表示します)**

Use Preservation Lock to restrict changes to retention policies and retention label policies Important Currently, adaptive policy scopes don't support Preservation Lock.

Reference:

https://learn.microsoft.com/en-us/purview/retention-preservation-lock

質問: **19**

Microsoft 365 サブスクリプションをお持ちです。

サブスクリプション用の暗号化メールをカスタマイズする必要があります。ソリューションは以下の要件を満たす必要があります。

暗号化された電子メールを送信するときは、電子メールに会社のロゴが含まれていることを確認します。

管理の手間を最小限に抑えます。

どの PowerShell コマンドレットを実行する必要がありますか?

A. Set-IRMConfiguration

B. Set-OMEConfiguration

C. Set-RMSTemplate

D. 新しいOME構成

正解: **(正解を表示します)**

To customize encrypted email in Microsoft 365, including adding a company logo, you need to modify the Office Message Encryption (OME) branding settings. The Set-OMEConfiguration PowerShell cmdlet allows you to configure branding elements such as:

Company logo

Custom text

Background color

This cmdlet is used to update existing OME branding settings, ensuring that encrypted emails sent from your organization include the required customizations.

質問: **20**

ホットスポットに関する質問

User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Microsoft Purview Data Security Posture Management for AI (DSPM for AI) を展開します。

User1 が次のアクションを実行できることを確認する必要があります。
- 「推奨事項」ページから推奨事項を表示します。
- アクティビティ エクスプローラーを使用して、すべてのイベントのユーザー リスク レベルを表示します。
ソリューションは最小権限の原則に従う必要があります。
各アクションに対して User1 をどのロール グループに追加する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Explanation:
Box 1: The Insider Risk Management Investigators role allows users to view recommendations related to insider risk cases and Microsoft Purview DSPM for AI insights. This role is appropriate because it grants access to review AI-related risk recommendations without unnecessary administrative privileges.
Box 2: The Insider Risk Management Analysts role allows users to analyze user risk levels and events using Activity Explorer. This follows the principle of least privilege, ensuring that User1 can only view risk levels and investigate but does not gain full administrative control over insider risk policies.

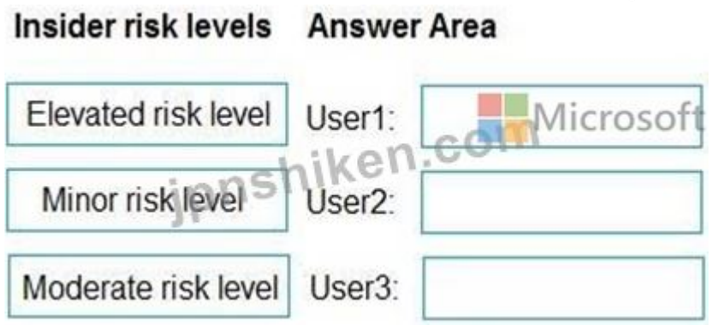
質問: **21**
トレーニング可能な分類子に基づく機密情報タイプがあります。
トレーニング可能な分類器の結果に満足していません。
分類器を再トレーニングする必要があります。
Microsoft Purview ポータルでは何を使用すればよいですか?
A. データ分類からのコンテンツエクスプローラー
B. 情報ガバナンスからのラベル
C. コンテンツ検索
D. 情報保護からのラベル
正解: **(正解を表示します)**

質問: **22**
デバイスの場所にデータ損失防止(DLP)ポリシーが適用されています。このポリシーは、米国のパスポート番号を含む文書を保護します。
ユーザーからは、ポリシーのせいで旅行管理 Web サイトにドキュメントをアップロードできないという報告があります。
ユーザーが旅行管理 Web サイトにドキュメントをアップロードできることを確認する必要があります。
ソリューションでは、保護されたコンテンツが他の場所にアップロードされるのを防ぐ必要があります。
どの Microsoft 365 エンドポイント データ損失防止 (エンドポイント DLP) 設定を構成する必要がありますか?
A. サービスドメイン
B. 許可されていないアプリ
C. 許可されていないブラウザ
D. ファイルパスの除外
正解: **(正解を表示します)**
You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.
- If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.
- If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using

質問: **23**
User1 という名前のユーザーを含む Microsoft 365 サブスクリプションがあります。
Label1 という名前の、極めて機密性の高い機密ラベルを作成します。
User1 が Microsoft 365 Copilot を使用して Label1 が適用されたコンテンツを要約できないようにする必要があります。このソリューションでは、User1 がコンテンツに直接アクセスできるようにする必要があります。
どのようなタイプのポリシーを作成する必要がありますか?
A. コミュニケーションコンプライアンス
B. 保持
C. データ損失防止 (DLP)
D. インサイダーリスク管理

正解: **C** (コメントを発表する)
To prevent a specific user from using M365 Copilot to summarize content with a "Highly Confidential" label, while allowing them direct access, you use a Microsoft Purview Data Loss Prevention (DLP) policy targeting Copilot, configured to block processing of that specific label for that user, without removing their underlying file permissions. This DLP policy intercepts Copilot's attempts to use the labeled content for summarization, effectively removing the content extraction right for Copilot in that scenario.
How it Works:
The DLP policy overrides Copilot's ability to extract and summarize content from files with the
"Highly Confidential" label when that specific user prompts Copilot.
This doesn't remove the user's direct permissions to open, read, or edit the file; it only stops Copilot from using it as a source for summaries.
This method leverages Purview DLP to create fine-grained controls over what Copilot can process, even when standard permissions allow access.
Reference:
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy

質問: **24**
ドラッグアンドドロップの質問
Microsoft Purview インサイダー リスク管理を使用し、User1、User2、User3 という名前の 3 人のユーザーが含まれる Microsoft 365 5 サブスクリプションがあります。
すべてのインサイダー リスク管理ポリシーでは、適応型保護が有効になっており、インサイダー リスク レベルの既定の条件が構成されています。
ユーザーが次のアクティビティを実行すると、インサイダー リスク ポリシー アラートがトリガーされます。
- User1 は、重大度の高いリスク スコアをもたらすデータ窃盗アクティビティを少なくとも 1 つ実行します。
- ユーザー 2 は、7 日以内に少なくとも 3 つの危険なユーザー アクティビティを実行し、それぞれが高重大度リスク スコアをもたらします。
- User3 は 7 日以内に少なくとも 2 回のデータ窃盗アクティビティを実行し、それぞれ重大度の高いリスク スコアが発生します。
各ユーザーにはどのインサイダーリスクレベルが割り当てられていますか？ 適切なレベルを適切なユーザーにドラッグしてください。各レベルは1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:
Box 1: Minor risk level

User1 performs at least one data exfiltration activity that results in a high severity risk score.
Minor:
This is the lowest risk level, assigned to users with low-severity alerts or those with at least one high-severity exfiltration activity.
Box 2: Elevated risk level
User2 performs at least three risky user activities within seven days, that each results in a high severity risk score.
Elevated:
This is the highest risk level, assigned to users with high-severity alerts, multiple high-severity insights, or confirmed high-severity alerts.
Box 3: Moderate risk level
User3 performs at least two data exfiltration activities within seven days, that each results in a high severity risk score.
Moderate:
This level indicates a medium risk, assigned to users with medium-severity alerts or those with at least two high-severity exfiltration activities.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-adaptive-protection

質問**: 25**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、『サインイン』ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、『パスワードを入力』ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL 『https://admin microsoft.com』を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク1
SharePoint Online サイトに保存されている製品情報を含むファイルをユーザーが手動で分類できるようにする必要があります。ソリューションは以下の要件を満たす必要があります。
- ユーザーは、ファイルに Product1 の分類を適用できる必要があります。
- 認証されたすべてのユーザーは、Product1 として分類されたファイルを開くことができる必要があります。
- Product1 として分類されるファイルは暗号化する必要があります。
正解**:**
Restrict access to content by using sensitivity labels to apply encryption When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:
* Only users within your organization can open a confidential document or email.
* Etc.
How to configure a label for encryption
Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels Step 2: Locate and select label Product1.
Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published:



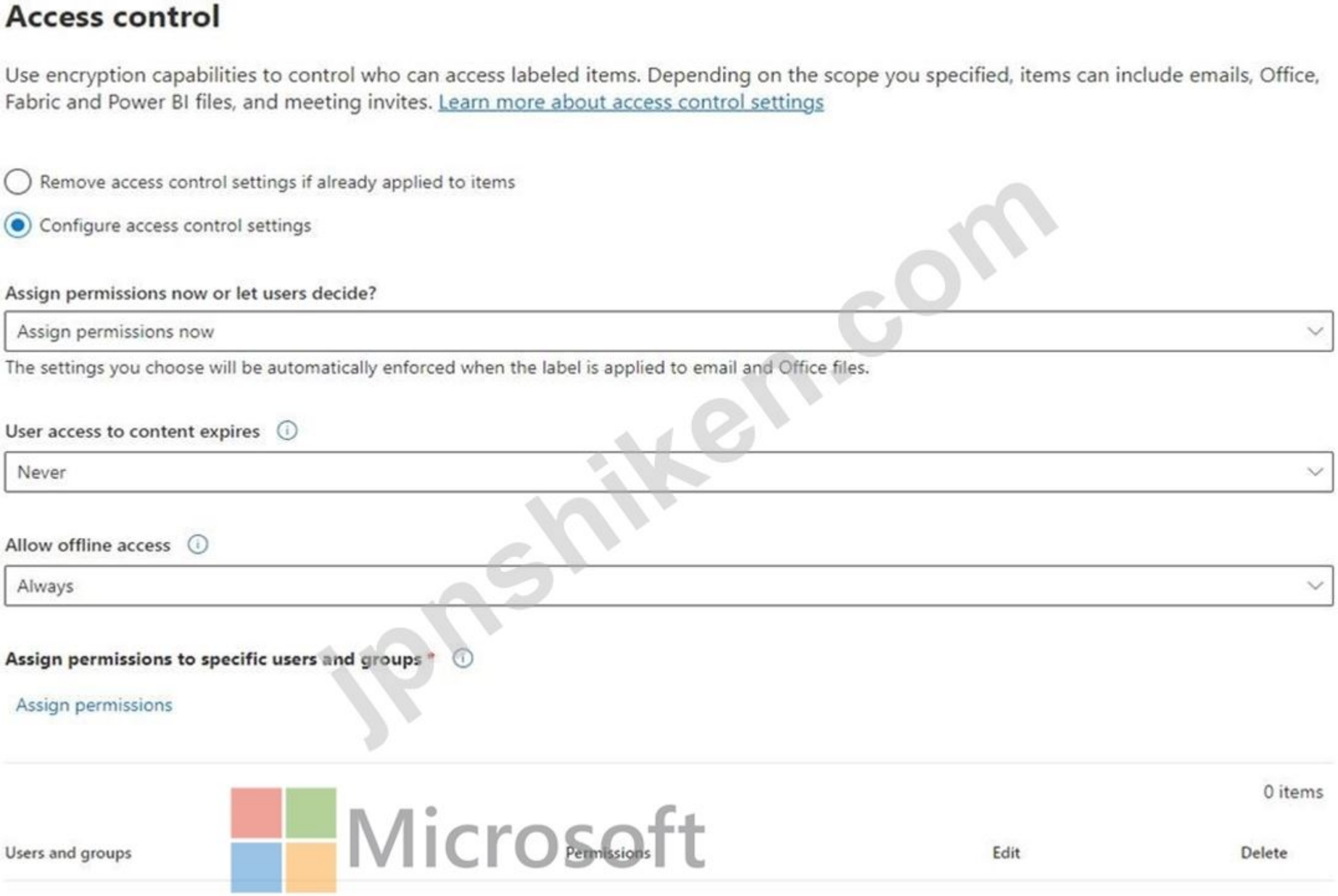
Step 4: Select Items, and Files. Deselect the other options.

Step 5: Then, on the Choose protection settings for the types of items you selected page, make sure you select Control access.



jpnshiken.com
Microsoft

Step 6: On the Access control page, select Configure access control settings: Turns on encryption with rights management and makes the following settings visible:



Step 7: Assign permissions to specific users or groups. Add users or groups Step 7a: For users: Any authenticated users.
Step 7b: Permissions: Select View
Note: You can grant permissions to specific people so that only they can interact with the labeled content:
1. First, add users or groups that will be assigned permissions to the labeled content.
2. Then, choose which permissions those users should have for the labeled content.
Assigning permissions:

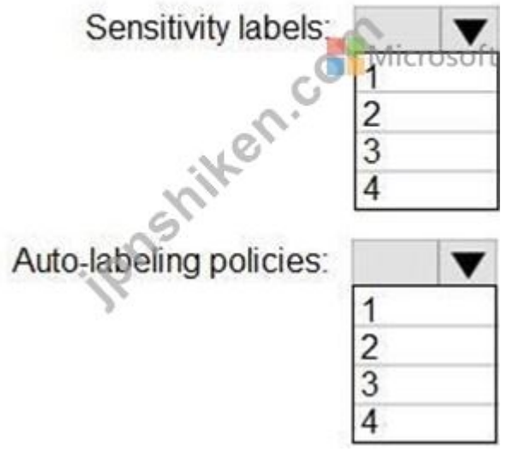


Microsoft
jpnshiken.com

Step 8: Click Save
Reference:
https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with
https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels

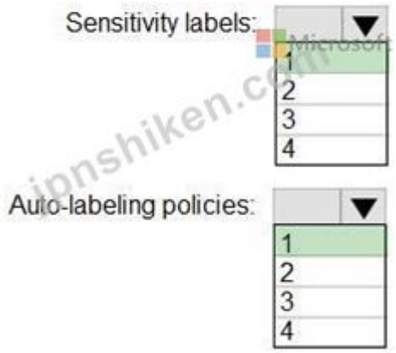
質問: **26**
ホットスポットに関する質問
次の要件を満たす情報コンプライアンス ポリシーを実装する必要があります。
- 米国のパスポート番号が記載された書類、
ドイツ、オーストラリア、日本は自動的に識別される必要があります。
- ユーザーが、
パスポート番号を入力すると、ユーザーはMicrosoftのツールヒントを受け取る必要があります
見通し。
- ユーザーはMicrosoft SharePoint Onlineまたは
OneDrive for Businessでパスポートを含む文書を共有する
番号。
作成する必要がある機密ラベルと自動ラベル付けポリシーの最小数はいくつですか?
回答するには、回答エリアで適切なオプションを選択してください。

Answer Area



正解:

Answer Area



Explanation:

Box 1: 1

We have four different kind of built-in sensitive information types for United States, Germany, Australia, and Japan in Data classification.

Box 2: 1

One Autolabeling policy can include all (4) passport sensitive information types in Rule- Conditions. In the same policy you choose one sensitivity label to add to files.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels

質問**: 27**

Microsoft 365 E5 サブスクリプションをお持ちです。

次の場所に対して静的保持ポリシーを作成する必要があります。

チームチャット

Exchangeメール

SharePoint サイト

Microsoft 365 グループ
Teams チャネル メッセージ
必要な保持ポリシーの最小数はいくつですか?
A. 1
B. 2
C. 3
D. 4
E. 5
正解: (正解を表示します)
If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations.
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365- worldwide&tabs=teams-retention#create-and-configure-a-retention-policy

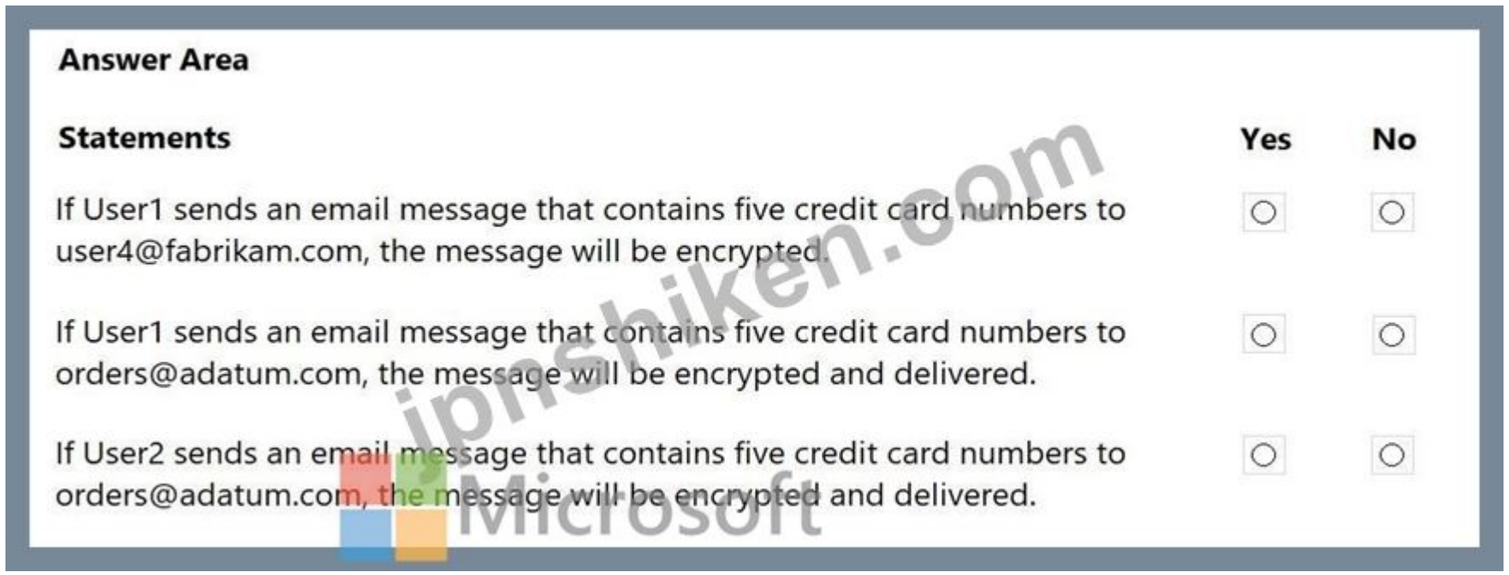
質問: **28**
ホットスポットに関する質問
次の表に示すユーザーを含む Microsoft 365 サブスクリプションがあります。

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

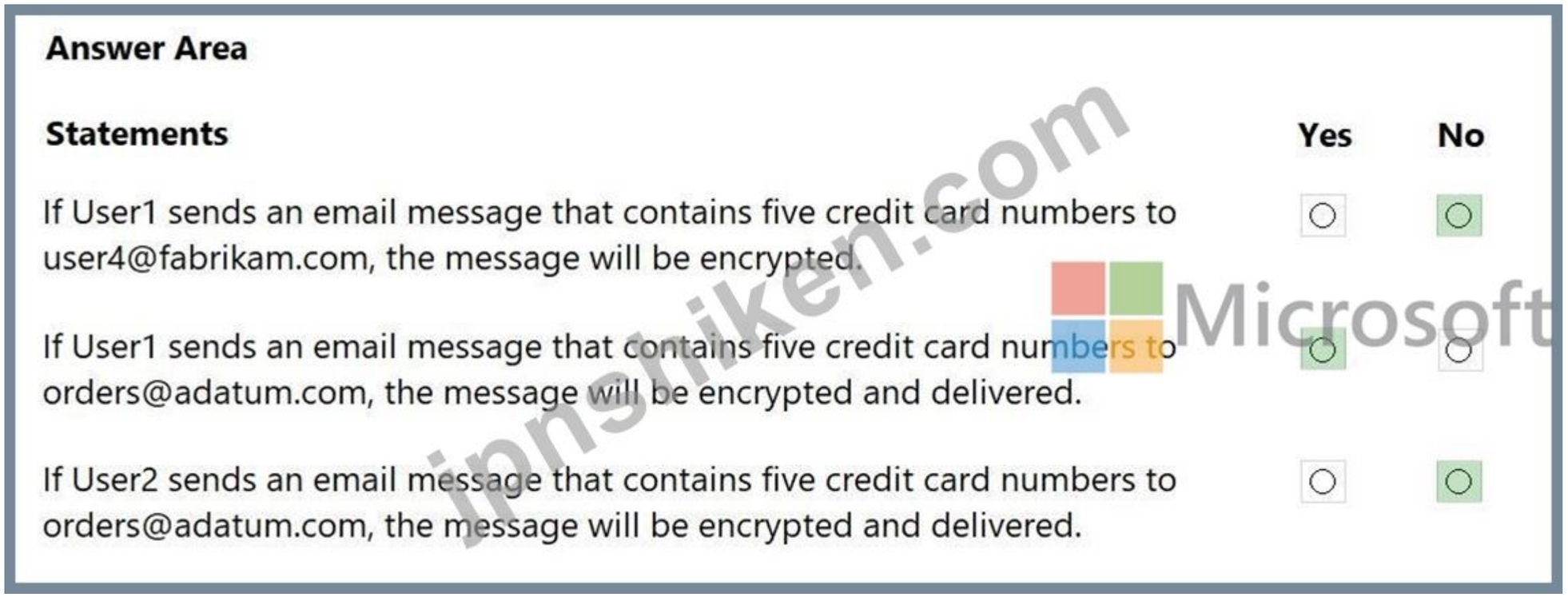
次の表に示すデータ損失防止 (DLP) ポリシーを作成します。

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	*None*	Send an incident report to the administrator.	*None*

jpnshiken.com Microsoft
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Box 1: No

Policy1 will be applied. Policy1 has an exception for user4@fabrikam. The processing is stopped at Policy1.

Note: Data loss prevention (DLP) policies are processed in a specific order. This process is called policy precedence. The policy with the lowest priority number is processed first. The first rule is configured as a priority "0" by default, the next one as "1", and so on.

Conditions are inclusive and are where you define what you want the rule to look for and context in which those items are being used.

Box 2: Yes

Policy1 will be applied.

Box 3: No
Policy2 will be applied.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference

質問: **29**
Microsoft 365 E5 テナントがあります。
データ損失防止 (DLP) ポリシーを作成します。
ポリシーによって Microsoft Teams チャット セッション内のドキュメントが保護されていることを確認する必要があります。
ポリシーで有効にする必要がある場所はどれですか?
A. SharePoint サイト
B. Teams チャットとチャネル メッセージ
C. Exchangeメール
D. OneDriveアカウント
正解: **D (**コメントを発表する**)**
Documents shared in Team Chats are stored in OneDrive and shared in Channel Chats are stored in SharePoint Sites.

質問: **30**
Microsoft 365 E5 サブスクリプションをお持ちです。
Label1 という名前の機密ラベルを作成し、Label1 をすべてのユーザーとグループに公開します。
コンピューター上に次のファイルがあります:
- ファイル1.doc
- ファイル2.docx
- ファイル3.xlsx
- ファイル4.txt
Label1 を適用できるファイルを特定する必要があります。
どのファイルを識別する必要がありますか?
A. File2.docxのみ
B. File2.docx と File3.xlsx のみ
C. File1.doc、File2.docx、File3.xlsxのみ
D. File1.doc、File2.docx、File3.xlsx、およびFile4.txt
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/purview/sensitivity-labels-office-apps#office-file-types-supported

質問: **31**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft SharePoint Online ドキュメントライブラリに Microsoft Word および Excel ドキュメントが含まれています。これらのドキュメントには、以下の種類の情報が含まれています。
- クレジットカード番号
- 英国内の住所
- 英国の国民保健サービス(NHS)の数字

- 次の単語を含むセンシティブなプロジェクト: プロジェクト
テイルスピン、プロジェクト コントソ、プロジェクト ファルコン
Microsoft Exchange Online には、次の種類の情報を含む電子メール メッセージがあります。
- クレジットカード番号
- ユーザーのサインイン資格情報
- 英国の国民保健サービス(NHS)の数字
コンプライアンス ポリシーに機密情報タイプ (SIT) を使用する予定です。
すべての情報タイプを分類するために必要な SIT の最小数はいくつですか?
A. 2
B. 5
C. 7
D. 10
正解**: B (**コメントを発表する**)**
* In Documents: Sensitive projects that contain the following words: Project Tailspin, Project Contoso, and Project Falcon - One SIT
* In documents: Physical addresses in the UK - one SIT
* Credit card numbers in documents and emails - one SIT
a single sensitive information type for credit card numbers can be applied to both documents and emails, often as part of a data loss prevention (DLP) or sensitivity labeling system in Microsoft 365 and other platforms. These systems can automatically detect credit card numbers within documents and emails and then apply predefined sensitivity labels that enforce security policies, such as encryption or access restrictions, for both types of content.
* User sign-in credentials in emails - one SIT
* National health service numbers from the UK in documents and emails - one SIT A single sensitive information type classification, such as for UK National Health Service (NHS) numbers, can be applied to both documents and emails, typically by using a data loss prevention (DLP) or sensitivity labelling system within Microsoft 365 or NHSmail. This allows a uniform policy to detect and protect NHS numbers whether they appear in a Word document or an email, ensuring consistent security protocols across different data formats within the NHS environment.
Reference:
https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード**: JPNshiken**」

質問**: 32**
次の図に示すように、エンドポイントに対してデータ損失防止 (DLP) ポリシーが構成されています。

Create rule

Use actions to protect content when the conditions are met.

Audit or restrict activities on devices

When specified activities are detected on devices for files containing the sensitive info you're protecting, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction.
Learn more restricting device activity

Service domain and browser activities

Detects when protected files are blocked or allowed to be uploaded to cloud service domains based on the 'Allow/Block cloud service domains' list in endpoint DLP settings.

- [x] Upload to a restricted cloud service domain or access from an unallowed browsers — Block

File activities for all apps

Decide whether to apply restrictions for file related activity. Unless you choose different restrictions for restricted apps or app groups below, any restrictions you choose here will be enforced for all apps.

- ( ) Don't restrict file activity
- (•) Apply restrictions to specific activity

When the activities below are detected on devices for supported files containing sensitive info that matches this policy's conditions, you can choose to audit the activity, block it entirely, or block it but allow users to override the restriction

- [x] Copy to clipboard — Audit only
- [x] Copy to a USB removable media — Audit only
- [x] Copy to a network share — Audit only
- [x] Print — Audit only

Save Cancel

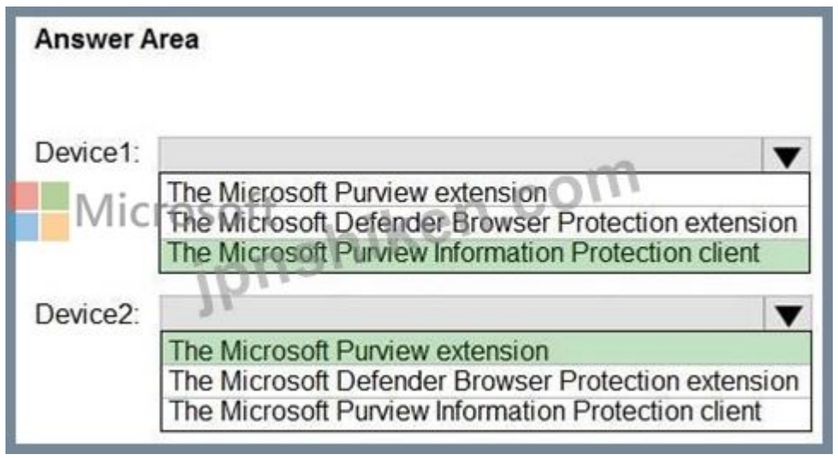
Microsoft jpnshiken.com

Computer1というコンピュータから、クラウドサービスにファイルをアップロードできる場合とできない場合があります。他のユーザーでも同じ問題が発生しています。
この問題の原因として考えられる 2 つのことは何ですか? それぞれの正解は完全な解決策を示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. Microsoft 365 エンドポイントのデータ損失防止 (エンドポイント DLP) 設定で許可されていないブラウザーが構成されていません。
B. Microsoft 365 エンドポイントのデータ損失防止 (エンドポイント DLP) 設定には、ファイル パスの除外があります。
C. 制限されたアプリによるアクセスアクションが監査のみに設定されています。
D. クリップボードにコピーするアクションが監査のみに設定されています。
E. コンピューターは Microsoft Purview にオンボードされていません。
正解: **(**正解を表示します**)**
Detects when a user attempts to upload an item to a restricted service domain or access an item through a browser. If they are using a browser that is listed in DLP as an unallowed browser, the upload activity will be blocked and the user is redirected to use Microsoft Edge . Microsoft Edge will then either allow or block the upload or access based on the DLP policy configuration
So if unallowed browser is NOT configured you can use chrome/etc with impugnity anc won't be kicked over to edge which observes the DLP policy, in other words, sometimes can upload (chrome), sometimes can not (edge).

質問: **33**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションがあり、このサブスクリプションには Device1 と Device2 という 2 台の Windows デバイスが含まれています。Device1 の既定のブラウザーは Microsoft Edge に設定されています。Device2 の既定のブラウザーは Google Chrome に設定されています。
ユーザーがデフォルトのブラウザーを使用して USB デバイスにファイルをコピーするときに、Microsoft Purview インサイダー リスク管理が信号を収集できるようにする必要があります。
各デバイスに何を展開する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Box 1: The Microsoft Purview Information protection client

Device1 has the default browser set to Microsoft Edge.

The Microsoft Purview Information Protection client, now integrated with Microsoft Edge, enables organizations to apply data security policies and protect sensitive information within the browser.

Specifically, Microsoft Purview Information Protection features like sensitivity labels and data loss prevention (DLP) can be leveraged in Edge for Business to control access and usage of sensitive documents and data.

Box 2: Microsoft Purview extension

Device2 has the default browser set to Google Chrome.

After the installation of the Microsoft Purview extension for Google Chrome, on Windows devices, organizations get the ability to also monitor attempts to access or upload sensitive items to a Cloud service when using the Google Chrome browser, and to actually enforce protective actions via data loss prevention.

The Microsoft Purview extension is used with Google Chrome, but it's not required for Microsoft Edge because Edge has built-in Endpoint DLP capabilities. The extension enhances data loss prevention for non-native applications, particularly for Chrome and other browsers where DLP needs to be explicitly extended.

Reference:

https://learn.microsoft.com/en-us/purview/dlp-chrome-get-started

質問: 34

ホットスポットに関する質問

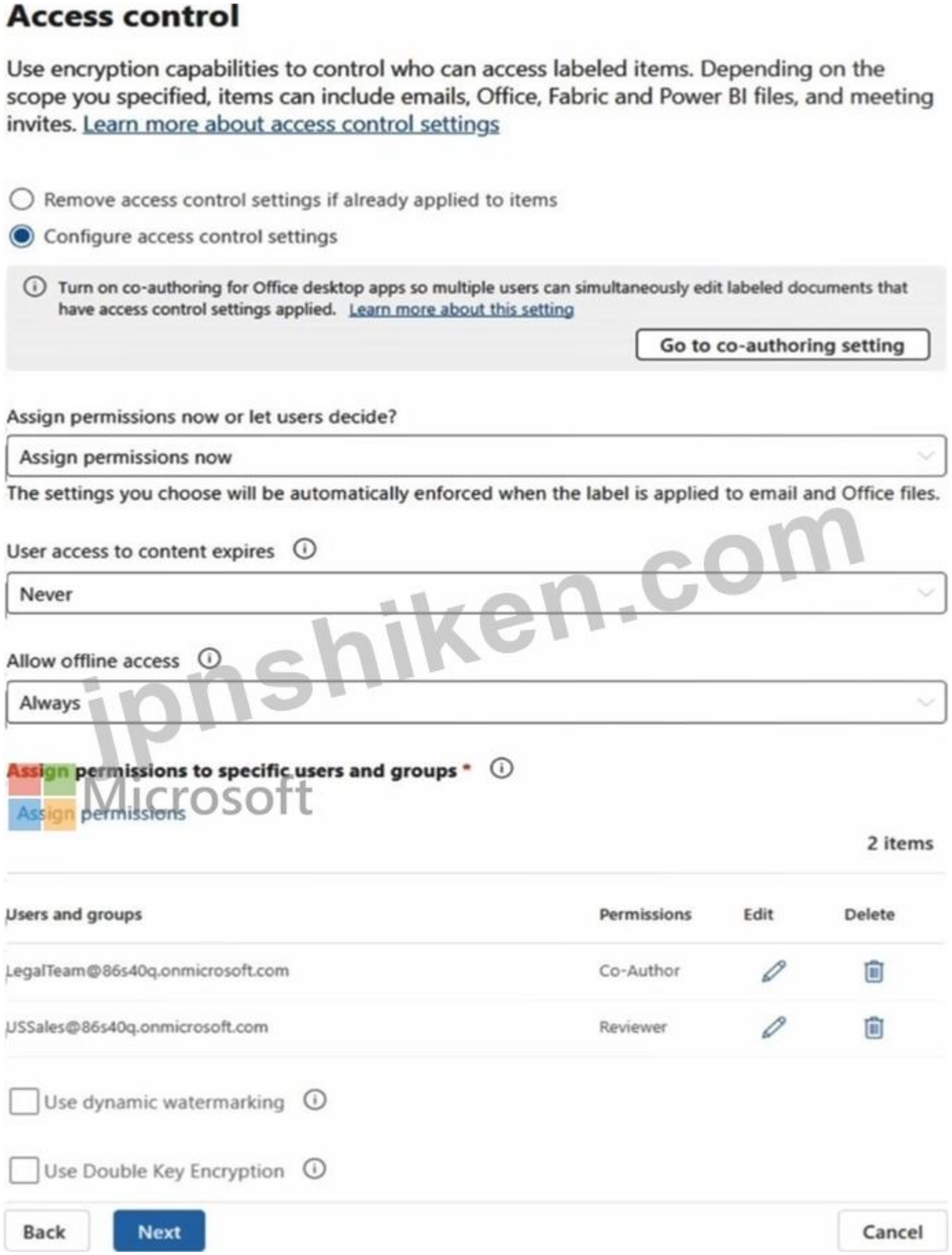
ドメイン名が 86s40q.onmicrosoft.com である Microsoft 365 E5 テナントがあります。

テナントには次の表に示すユーザーが含まれます。

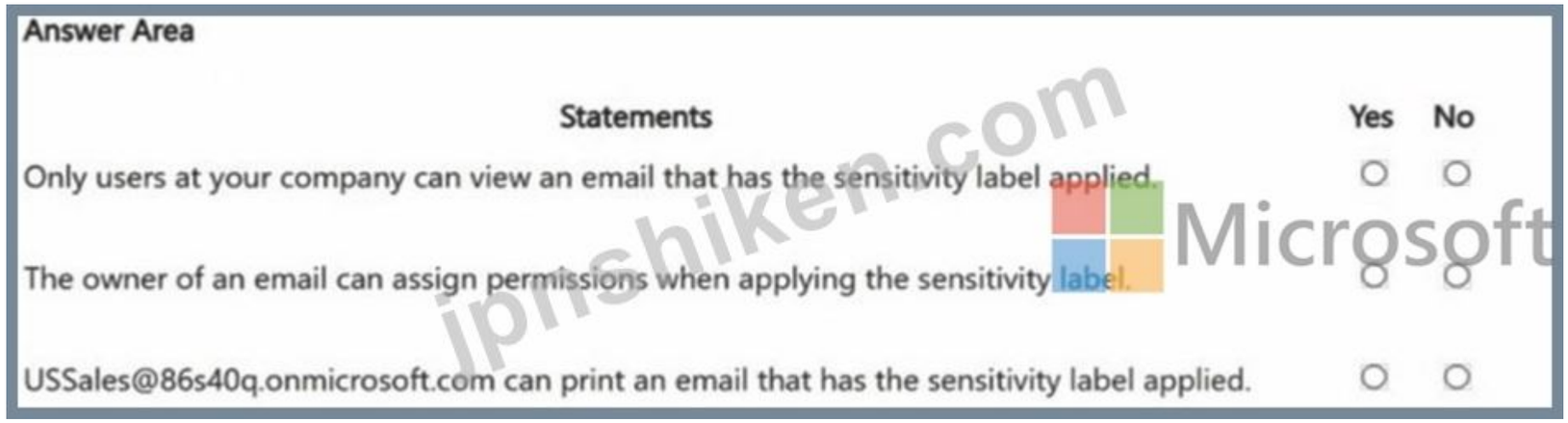
Name	User type
User1	Member
User2	Guest

公開された機密ラベルがあります。

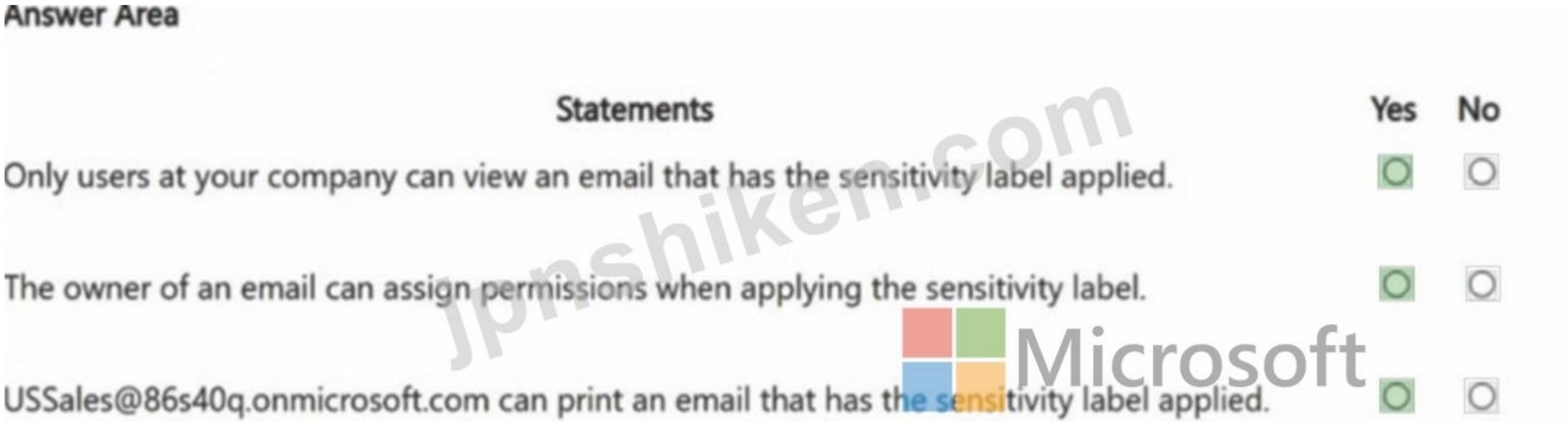
機密ラベルのアクセス制御設定は、図に示すように構成されています。(図タブをクリックします。)



以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



質問: **35**
機密情報の種類に使用される単語のリストを含む電子メールを受信します。
キーワード辞書のソースとして使用できるファイルを作成する必要があります。
リストはどの形式で保存すればよいですか?
A. 各単語の要素を持つJSONファイル
B. 各行に1つの単語が含まれるDOCXファイル
C. カンマで区切られた単語を含むCSVファイル
D. Dictionaryという名前のテーブルを含むACCDBデータベースファイル
正解: **(**正解を表示します**)**
Correct:
* a CSV file that contains words separated by commas
* a text file that has one word on each line
Incorrect:
* an ACCDB database file that contains a table named Dictionary

* a DOCX file that has one word on each line
* a JSON file that has an element for each word
* a TSV file that contains words separated by tabs
* an XML file that contains a keyword tag for each word
* an XLSX file that contains one word in each cell of the first row
Note:
To create a keyword dictionary for a sensitive information type in Microsoft Purview Data Loss Prevention (DLP), you must use a plain text (.txt) file (or a .CSV file) where each keyword is on a separate line.
Format Example (TXT file):
confidential
sensitive
classified
top secret
This format is simple, efficient, and directly compatible with Microsoft 365 DLP policies for keyword dictionaries.
How to use the keyword dictionary?
Create a text file with one keyword per line.
Upload it to Microsoft Purview under Data Classification > Sensitive Info Types.
Use the dictionary in a DLP policy to identify and protect sensitive information.
In steps:
Create a keyword dictionary using the Microsoft Purview portal
Use these steps to create or import keywords for a custom dictionary:
1. Sign in to the Microsoft Purview portal Information Protection > Classifiers > Sensitive info types.
2. Select + Create sensitive info type and then enter a Name and Description for your sensitive info type. Choose Next.
3. On the Define patterns for this sensitive info type page, choose + Create pattern.
4. In the New pattern window, select a Confidence level.
5. Choose Add a Primary element and select Keyword dictionary.
*-> 6. On the Add a keyword dictionary flyout, you can:
6a. Upload a dictionary file in TXT or CSV format.
6b. Choose from existing dictionaries.
or create a new dictionary by entering keywords manually and giving it a name.
Reference:
https://learn.microsoft.com/en-us/purview/sit-create-a-keyword-dictionary

質問: 36
プロジェクトの終了時に、多数のファイルを含むMicrosoft SharePoint Onlineライブラリにプロジェクトドキュメントをアップロードします。以下は、プロジェクトドキュメントのファイル名の例です。
- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx

この命名形式を使用するすべてのドキュメントには、プロジェクト ドキュメントというラベルを付ける必要があります。
自動適用保持ラベル ポリシーを作成する必要があります。
ファイルを識別するには何を使用すればよいですか?
A. 学習可能な分類器
B. 保持ラベル
C. 機密情報の種類
正解: **(**正解を表示します**)**

質問: **37**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft SharePoint Online で機密ラベルのサポートを有効にする必要があります。
何を使うべきでしょうか?
A. Microsoft Purview ポータル
B. Microsoft Entra 管理センター
C. SharePoint 管理センター
D. Microsoft 365 管理センター
正解: **C (**コメントを発表する**)**
To enable support for sensitivity labels in Microsoft SharePoint Online, you must configure the setting in the SharePoint admin center.
Sensitivity labels in SharePoint Online allow labeling and protection of files stored in SharePoint and OneDrive. This feature must be enabled in the SharePoint admin center # Settings # Information protection to allow sensitivity labels to apply encryption and protection to stored documents.

質問: **38**
あなたの会社は Microsoft 369 E5 サブスクリプションを所有しており、Microsoft Purview Advanced Message Encryption を使用する予定です。
社内の各製品グループでは、暗号化された電子メールに標準の Microsoft 365 ロゴではなく、個別の製品ロゴを表示する必要があります。
ブランディング テンプレートを作成するにはどうすればよいでしょうか?
A. RMS テンプレートを作成します。
B. トランスポート ルールを作成します。
C. New-OMEConfigurationコマンドレットを実行します。
D. Set-IRMConfigurationコマンドレットを実行します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to- encrypted-messages

質問: **39**
Microsoft Teams を使用する Microsoft 365 E5 サブスクリプションがあります。
機密ラベルを実装する予定です。
新しい Microsoft Teams サイトに機密ラベルを表示および適用できることを確認する必要があります。
まず何をすべきでしょうか?
A. Set-SPOSiteコマンドレットを実行します。
B. Microsoft Entra ID で EnableMIPLabels 設定を構成します。
C. Execute-AzureAdLabelSync コマンドレットを実行します。

D. グループとサイトを対象とする新しい機密ラベルを作成します。
正解: **B** (コメントを発表する)

質問: **40**
ドラッグアンドドロップの質問
自動適用保持ラベル ポリシーの条件として使用できるトレーニング可能な分類子を作成する必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Microsoft
ipnshiken.com

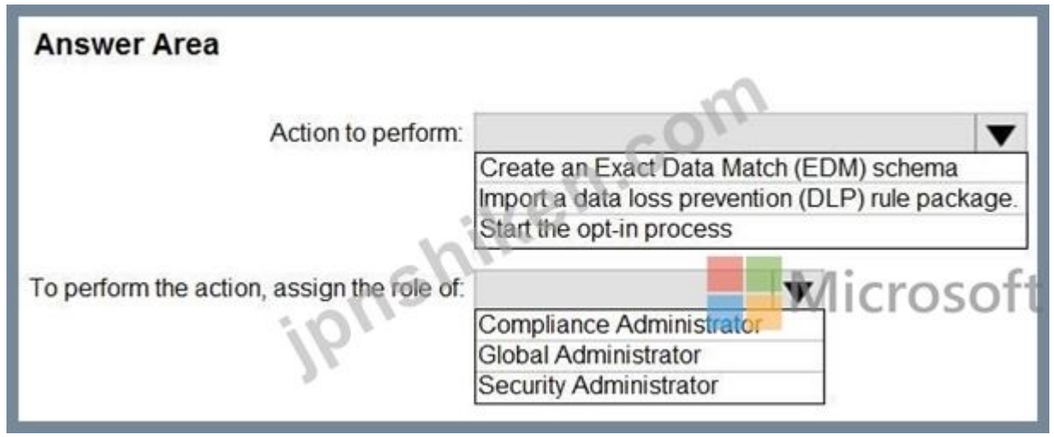
正解:



Microsoft
jpnshiken.com

Explanation:
To create a trainable classifier that can be used in an auto-apply retention label policy, you need to follow these key steps:
1. Create the trainable classifier
This is the first step where you define the classifier, specifying the types of content it should identify.
2. Test the trainable classifier
Before using the classifier in production, you need to validate its accuracy by testing it against sample documents to ensure it correctly classifies the intended data.
3. Publish the trainable classifier
Once testing is successful, you must publish the classifier so that it can be used in policies like auto-apply retention labels in Microsoft Purview.

質問**: 41**
ホットスポットに関する質問
新しい Microsoft 365 E5 テナントがあります。
製品注文フォームを検出する、カスタムのトレーニング可能な分類器を作成する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
まず何をすべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



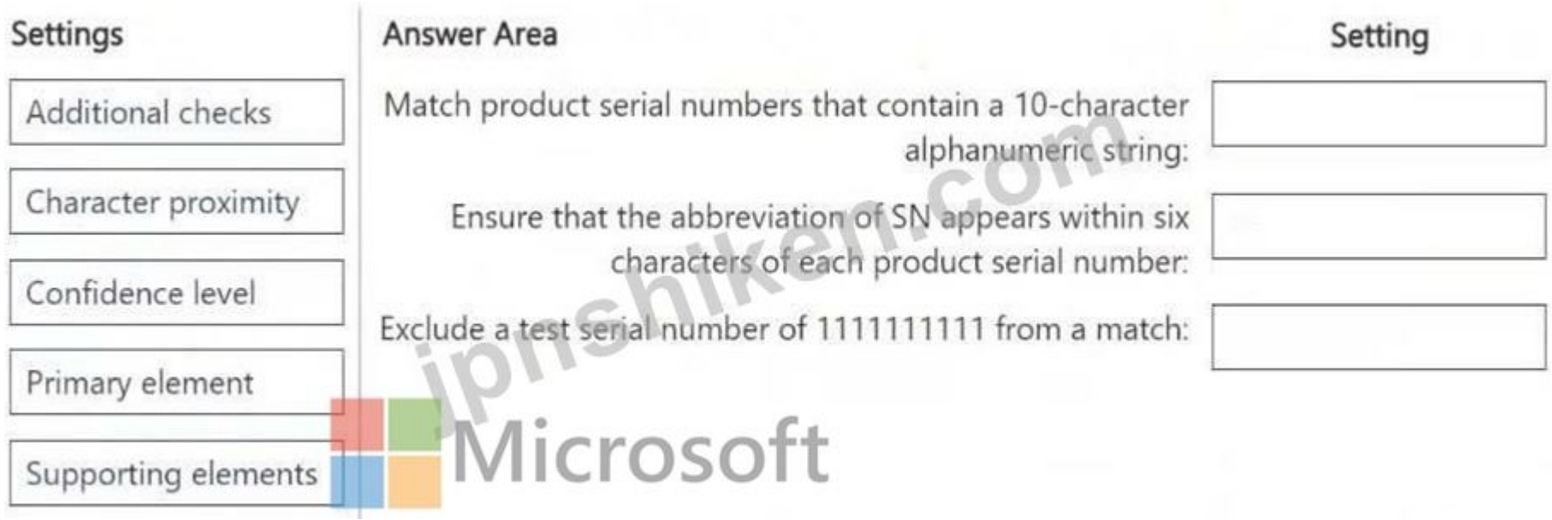
正解:

Answer Area

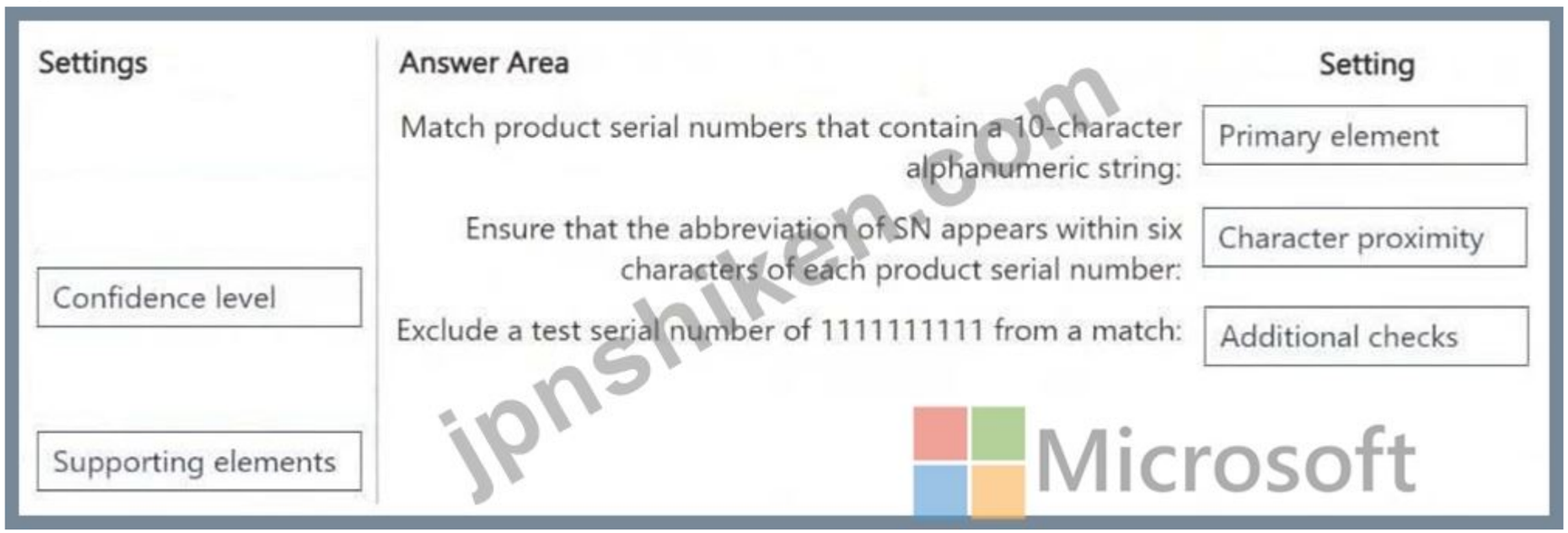


Explanation:
The opt-in can't be performed by the Compliance Administrator, the GA is required:
"To access classifiers in the UI:
the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier."
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started- with?view=o365-worldwide

質問: **42**
ドラッグアンドドロップの質問
データ損失防止 (DLP) が実装された Microsoft 365 E5 サブスクリプションがあります。
カスタムの機密情報タイプを作成する必要があります。ソリューションは以下の要件を満たす必要があります。
- 10 文字の英数字文字列を含む製品シリアル番号を一致させます。
- SNの略語が6文字以内であることを確認してください。
各製品のシリアル番号。
- テストシリアル番号 1111111111 を一致から除外します。
各要件に対してどのパターン設定を行うべきでしょうか？適切な設定を正しい要件にドラッグしてください。各設定は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Microsoft custom sensitive info types use pattern settings to refine detection accuracy for data loss prevention (DLP) policies.

The Primary element defines the main pattern that must be detected. Since we need to match a 10-character alphanumeric string, this should be defined in the primary element.

Character proximity determines how close a supporting keyword (e.g., "SN") must be to the detected data. Since "SN" must be within six characters of the product serial number, this setting ensures a valid match.

Additional checks allow for exceptions and exclusions in the detection logic. This ensures that 1111111111 (a test serial number) is excluded from triggering a match.

質問: 43

ホットスポットに関する質問

Microsoft 365 E5 サブスクリプションをお持ちです。

次の図に示すように、Scope1 という名前の適応スコープを作成します。



Scope1 を含む Policy1 という名前の保持ポリシーを作成します。
ポリシー 1 を適用できる 3 つの場所はどれですか。回答するには、回答領域で適切な場所を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

jpnshiken.com

Answer Area

Choose locations to apply the policy

Based on the scopes you added, this policy can be applied to content in these locations.

Status	Location
Off	Exchange email
Off	SharePoint sites
Off	OneDrive accounts
Off	Microsoft 365 Groups
Off	Skype for Business
Off	Teams channel messages
Off	Teams chats
Off	Teams private channel messages
Off	Yammer community messages
Off	Yammer user messages

正解:

Answer Area

Choose locations to apply the policy

Based on the scopes you added, this policy can be applied to content in these locations.

Status	Location
Off	Exchange email
Off	SharePoint sites
Off	OneDrive accounts
Off	Microsoft 365 Groups
Off	Skype for Business
Off	Teams channel messages
Off	Teams chats
Off	Teams private channel messages
Off	Yammer community messages
Off	Yammer user messages

jpnshiken.com

Microsoft

Explanation:
A retention policy with an adaptive scope defined by the Microsoft 365 Groups type can be applied to Exchange email, SharePoint sites, and OneDrive accounts. However, the scope is most effective when applied to locations that are a part of the Microsoft 365 Group, such as the group's mailbox (Exchange email) and the group's associated SharePoint site, which includes its OneDrive for Business account.
Box 1: Exchange email
Box 2: SharePoint sites
Box 3: OneDrive accounts
How it works
Adaptive Scopes: These scopes are dynamic filters that automatically identify target locations for a retention policy.
Group Type Scope: When you use the "Microsoft 365 Groups" scope type, it targets content associated with a group, which includes:
The group's mailbox in Exchange.
The group's associated SharePoint site.
The group's associated OneDrive for Business account.
Application: The policy is automatically applied to all users and sites within the group, making it a scalable solution for managing retention across the group's entire ecosystem.
Flexibility: This is particularly useful for organizations where group membership and content locations change frequently, as the policy automatically adapts to these changes.
Reference:
https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

質問: 44
contoso.com という名前のドメインを使用する Microsoft 365 E5 テナントがあります。
User1 というユーザーは、Microsoft Purview Advanced Message Encryption を使用して暗号化されたリンクベースのブランド化された電子メールを、次の表に示す受信者に送信します。

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

User1 はどの受信者のメールを取り消すことができますか?
A. 受信者1のみ
B. 受信者4のみ
C. 受信者1と受信者2のみ
D. 受信者3と受信者4のみ
E. 受信者1、受信者2、受信者3、受信者4
正解: (正解を表示します)
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail

質問: 45
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、Microsoft Purview にオンボードされ、次の表のように構成されたデバイスが含まれています。

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

サブスクリプションには、次の表に示すユーザーが含まれます。

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

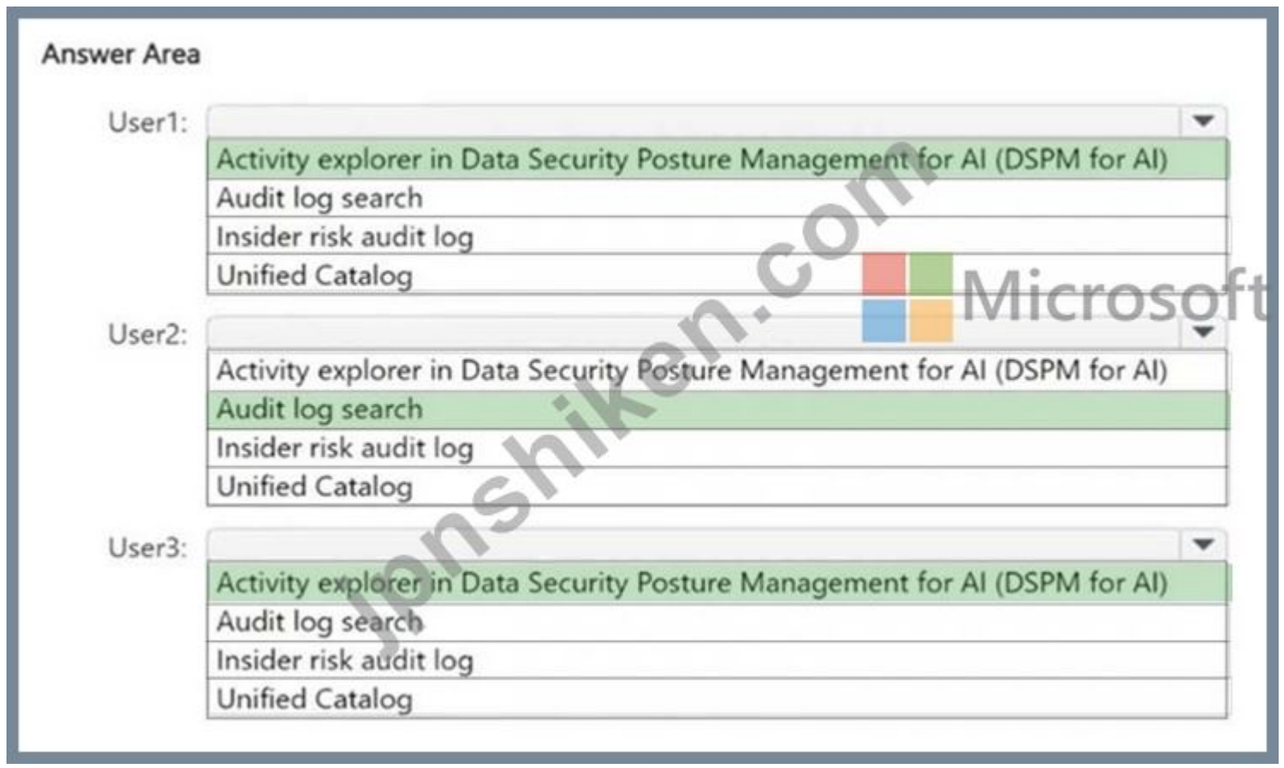
アクティビティを見直す必要があります。
各ユーザーには何を使用すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area

User1:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

User2:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

User3:
- Activity explorer in Data Security Posture Management for AI (DSPM for AI)
- Audit log search
- Insider risk audit log
- Unified Catalog

正解:



Explanation:

User1: Since the Microsoft Purview browser extension is installed on Device1, AI-related activity performed by User1 (generating an image using a generative AI website) can be reviewed in Activity explorer in DSPM for AI.

User2: Since Device2 does not have the Microsoft Purview browser extension installed, AI- related activity cannot be tracked in DSPM for AI. Instead, Audit log search should be used to review activity such as using Microsoft 365 Copilot.

User3: Since Device3 has the Microsoft Purview browser extension installed, AI-related activity (browsing sample content on a generative AI website) can be reviewed using Activity explorer in DSPM for AI.

質問**: 46**

Microsoft 365 E5 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトが含まれています。Site1 には、次の表に示すファイルが含まれています。

Name	Author
File1.docx	User1
File2.docx	User2
File3.docx	USER1

Microsoft Purview ポータルで、Content1 という名前のコンテンツ検索を作成し、次の図に示すように検索条件を構成します。



Content1 によって返されるファイルはどれですか?

A. File2.docxのみ

B. File3.docxのみ

C. File1.docx と File2.docx のみ

D. File1.docx と File3.docx のみ

E. Filet.docx、File2.docx、およびFile3.docx

正解: **(**正解を表示します**)**

Microsoft Purview, Keyword queries and search conditions for eDiscovery Values aren't case-sensitive. Both User1 (File1.docx) and USER1 (File3.docx) will match the Search condition - Author:USER1.

Reference:

https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**

User1 という名前のユーザーを含む Microsoft Entra テナントにリンクされた Microsoft 365 サブスクリプションがあります。

Microsoft 365 監査ログを検索する権限を User1 に付与する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。

ユーザーにどのロールを割り当てる必要がありますか?

A. Exchange 管理センターのコンプライアンス管理ロール

B. Microsoft Entra 管理センターのセキュリティ リーダーの役割
C. Exchange 管理センターの表示専用監査ログの役割
D. Microsoft Purview ポータルのレビュー担当者の役割
正解: (正解を表示します)

質問: **48**
ホットスポットに関する質問
Microsoft Exchange Online と Teams を使用する Microsoft 365 ES サブスクリプションがあります。
ユーザーがクラウド添付ファイルを含むメッセージを送信するときに、自動ラベル付けポリシーを使用して、クラウド添付ファイルに保持ラベルが適用されるようにする必要があります。
保持期間を開始するために保持ラベルをどのように構成すればよいですか。また、どの場所に自動ラベル付けポリシーを適用すればよいですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:
Answer Area



Explanation:
Box 1: Labeled
Automatically apply a retention label to retain or delete content

Auto-apply labels to cloud attachments
You might need to use this option if you're required to capture and retain all copies of files in your tenant that are sent over communications by users, or files that are referenced in Copilot for Microsoft 365. You use this option in conjunction with retention policies for the communication services themselves; Exchange, Teams, Viva Engage, and Copilot for Microsoft 365.
Important
When you select a label to use for auto-applying retention labels for cloud attachments, ensure that the label retention setting Start the retention period based on is When items were labeled.
Box 2: Microsoft 365 Group mailboxes & sites only
When you select a label to use for auto-applying retention labels for cloud attachments, make sure the label retention setting Start the retention period based on is When items were labeled.
When you configure the locations for this option, you can select:
* SharePoint classic and communication sites for shared files stored in SharePoint communication sites, team sites that aren't connected by Microsoft 365 groups, and classic sites.
*-> Microsoft 365 Groups for shared files that are stored in team sites connected by Microsoft 365 groups.
* OneDrive accounts for shared files stored in users' OneDrive.
Reference:
https://learn.microsoft.com/en-us/purview/apply-retention-labels-automatically

質問**: 49**
ケーススタディ 1 - Contoso 社
概要
Contoso 社は、モントリオールに本社を置き、シアトル、ボストン、ヨハネスブルグに 3 つの支社を持つコンサルティング会社です。
既存の環境
Microsoft 365 環境
Contoso 社には Microsoft 365 E5 テナントがあります。このテナントには、次の表に示す管理ユーザーアカウントが含まれています。

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

ユーザーは次の場所にデータを保存します。
- SharePoint サイト
- OneDriveアカウント
- Exchangeメール
- Exchangeパブリックフォルダ
- Teamsチャット
- Teams チャネル メッセージ
研究部門のユーザーが文書を作成する際は、各文書に10桁のプロジェクトコードを追加する必要があります。999で始まるプロジェクトコードは機密情報です。
SharePoint Online 環境
Contoso には、Site1、Site2、Site3、Site4 という名前の 4 つの Microsoft SharePoint Online サイトがあります。
Site2 には、次の表に示すファイルが含まれています。

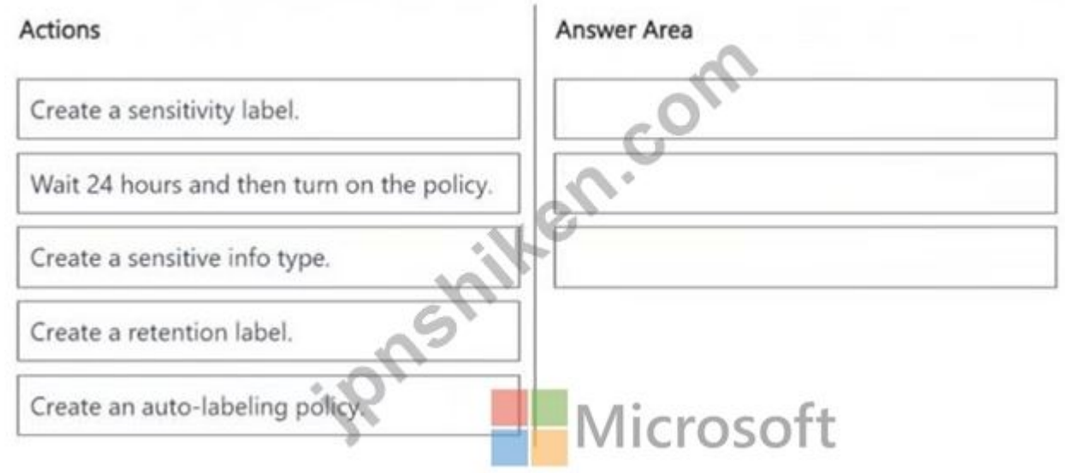
Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

次の表に示すように、User1 と User2 という名前の 2 人のユーザーに Site2 のロールが割り当てられています。

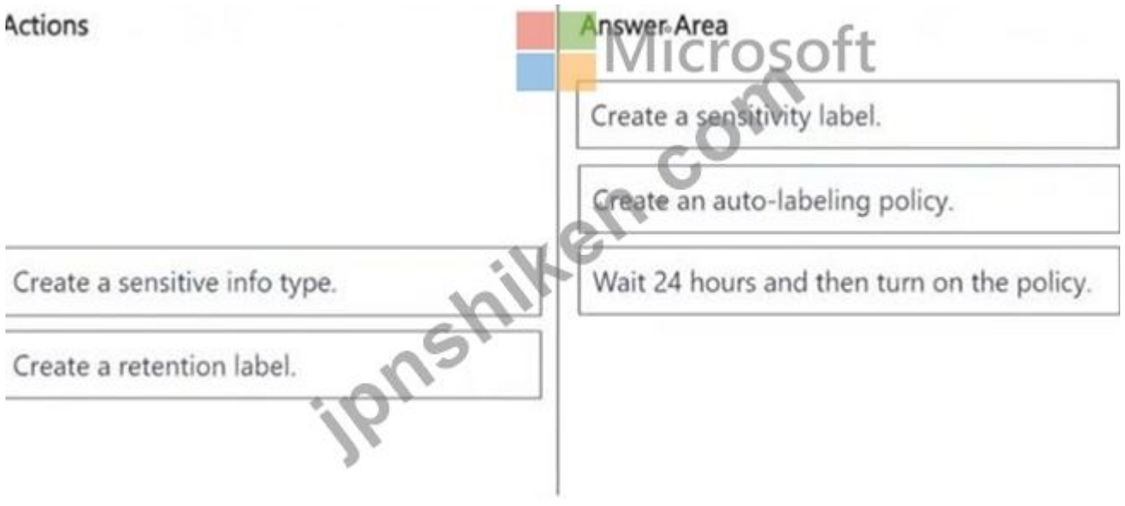
User	Role
User1	Site owner
User2	Site visitor

Site3には、会社のプロジェクトに関連する文書が保存されています。文書はプロジェクトごとにフォルダ階層に整理されています。
Site4 には次の 2 つの保持ポリシーが適用されています。
- 名前: Site4RetentionPolicy1
ポリシーを適用する場所: サイト4
2年以上前のアイテムを削除
コンテンツを削除する基準: アイテムが作成された日時
- 名前: Site4RetentionPolicy2
ポリシーを適用する場所: サイト4
特定の期間アイテムを保管する: 4 年間
保存期間の開始基準: アイテムが作成された日時
保存期間の終了時: 何もしない
問題ステートメント
Contoso社の経営陣はデータ漏洩を懸念しています。研究部門の機密文書が漏洩するケースが複数回発生しました。
要件
計画された変更
Contoso では、次のデータ損失防止 (DLP) ポリシーを作成する予定です。
- 名前: DLPpolicy1
ポリシーを適用する場所: サイト2
条件：
コンテンツには、次のいずれかの機密情報タイプが含まれています: SWIFT コード
- インスタンス数: 2〜任意
アクション: コンテンツへのアクセスを制限する
技術要件
Contoso は次の技術要件を満たす必要があります。
- すべての管理ユーザーは DLP レポートを確認できる必要があります。
- 可能な限り、最小権限の原則を使用する必要があります。
- すべてのユーザーについて、Microsoft 365のデータは少なくとも
1年。
- 機密文書は、以下の方法で検出し保護する必要があります。
マイクロソフト365。

- クレジットカード番号を含むサイト1文書にはラベルを付ける必要がある
自動的に。
- すべての管理ユーザーはMicrosoft 365を作成できる必要があります
機密ラベル。
- プロジェクトが完了したら、サイト3にある関連する文書は
プロジェクトは10年間保持する必要があります。
ドラッグアンドドロップの質問
Site1 ドキュメントの技術要件を満たす必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:
Create a retention label. -> Has nothing to do with information protection.
Create a sensitive info type. -> Not needed because for credit cards, there is a built-in one.

質問: **50**
Microsoft Teams チャネルの会話とプライベート チャットのすべてのファイルを保持するための保持ポリシーを作成する必要があります。
保持ポリシーではどの 2 つの場所を選択する必要がありますか? それぞれの正解は解決策の一部を示しています。

注意: 正しい選択ごとに 1 ポイントが加算されます。
A. Microsoft 365 グループ
B. Exchangeメール
C. チームチャンネルメッセージ
D. SharePoint サイト
E. OneDriveアカウント
F. チームチャット
正解**: (**正解を表示します**)**
To retain all files from Microsoft Teams channel conversations and private chats, you need to select three locations in a retention policy: Teams channel messages, Teams chats, and OneDrive for Business. Select "Teams channel messages" for files in channels, "Teams chats" for private and group chats, and "OneDrive for Business" for files shared in those private and group chats.
*-> Teams channel messages: This includes messages and files from standard and private channels.
*-> Teams chats: This covers messages and files from 1:1 and group chats (excluding private channels).
* OneDrive for Business: Files shared in private chats are stored in the OneDrive account of the user who shared them, so this location is necessary for retention.
Reference:
https://learn.microsoft.com/en-us/purview/create-retention-policies

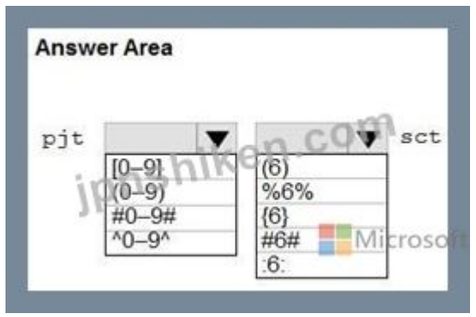
質問**: 51**
Microsoft 365 テナントがあります。
顧客の詳細を保存するデータベースがあります。各顧客には、数字と文字の固定パターンで構成される13桁の一意の識別子が割り当てられています。
次の要件を満たすデータ損失防止 (DLP) ソリューションを実装する必要があります。
単一の顧客識別子を含む電子メール メッセージは社外に送信できます。
2 つ以上の顧客識別子を含む電子メール メッセージは、会社のデータ プライバシー チームによって承認される必要があります。
解決策にはどの 2 つのコンポーネントを含める必要がありますか? それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. 機密ラベル
B. 機密情報の種類
C. DLPポリシー
D. 保持ラベル
E. メールフロールール
正解**: B,C (**コメントを発表する**)**
You need to define a custom sensitive information type that recognizes the unique 13-digit identifier format for customer records. Microsoft Purview DLP policies use these types to identify and protect sensitive data.
A Data Loss Prevention (DLP) policy is required to enforce the rules. It will allow emails with a single identifier but trigger an approval workflow when two or more identifiers are detected.

質問**: 52**
保持期間が 7 年間の保持ラベルを作成します。
クレジットカード番号が記載された文書は 7 年間保管する必要があります。
その他の文書は保管しないでください。
何を創造すべきでしょうか?

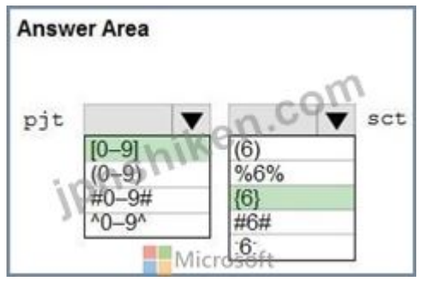
A. 自動適用タイプの保持ラベルポリシー
B. 公開タイプの保持ラベルポリシー
C. ファイルを自動的に削除する保持ポリシー
D. ファイルを自動的に保持する保持ポリシー
正解: (正解を表示します)
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically

質問: **53**
Microsoft 365 E5 サブスクリプションをお持ちです。
インサイダー リスク管理を使用して、法医学的証拠を収集および調査する予定です。
法医学的証拠のキャプチャを有効にする必要があります。
まず何をすべきでしょうか?
A. 情報保護スキャナーを構成します。
B. 優先ユーザー グループを作成します。
C. 容量を要求します。
D. アダプティブ保護を有効にします。
正解: (正解を表示します)

質問: **54**
ホットスポットに関する質問
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
「pjt」という文字で始まり、その後に6桁の数字が続き、「sct」という文字で終わるプロジェクトコードの内容を検出するには、機密情報タイプ(SIT)を作成する必要があります。以下はプロジェクトコードの例です。
pjt123456sct
正規表現をどのように完成させるべきでしょうか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:
Box 1: [0-9]
Pattern: [0-9]{0,3}
Interpretation: Look for zero to three occurrences of the decimal digits 0 through 9.
Box 2: {6}
Quantifiers
A quantifier specifies how many instances of the previous element (which can be a character, a group, or a character class) must be present in the input string for a match to occur. Quantifiers include the language elements listed in the following table.
Quantifier: { n }
Description: Matches the previous element exactly n times.
Pattern: ",\d{3}"
Matches: ",043" in "1,043.6", ",876", ",543", and ",210" in "9,876,543,210" Reference:
https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expressions
https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick- reference

質問: **55**
次の場所から 7 年後にコンテンツを削除するには、保持ポリシーを作成する必要があります。
* Exchange Online メール
* SharePoint Online サイト
* OneDriveアカウント
* Microsoft 365 グループ
* Teams チャネル メッセージ
* チームチャット
作成する必要がある保持ポリシーの最小数はいくつですか?
A. 1
B. 4
C. 3
D. 2
正解: (正解を表示します)

質問: **56**
Microsoft 365 サブスクリプションをお持ちです。
Microsoft Purview ポータルからコンテンツ検索を作成して実行します。
コンテンツ検索の結果をダウンロードする必要があります。

まず何を入手すべきでしょうか?
A. ピン
B. エクスポートキー
C. 証明書
D. パスワード
正解: **B** (コメントを発表する)

質問: **57**
ホットスポットに関する質問
次の表に示すファイルを含む、Site1 という名前の Microsoft SharePoint Online サイトがあります。

Name	Number of IP addresses in the file
File1.txt	2
File2.docx	6
File3.dat	4

次の表に示す高度な DLP ルールを持つ、DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

Name	Content contains	Policy tip	Priority
Rule1	1 or more IP addresses	Tip1	0
Rule2	2 or more IP addresses	Tip2	1
Rule3	6 or more IP addresses	Tip3	2

DLP1 を Site1 に適用します。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Answer Area

Statements	Yes	No
File1.txt has the Tip1 policy tip.	○	○
File2.docx has the Tip3 policy tip.	○	○
File3.dat has the Tip2 policy tip.	○	○

jpnshiken.com

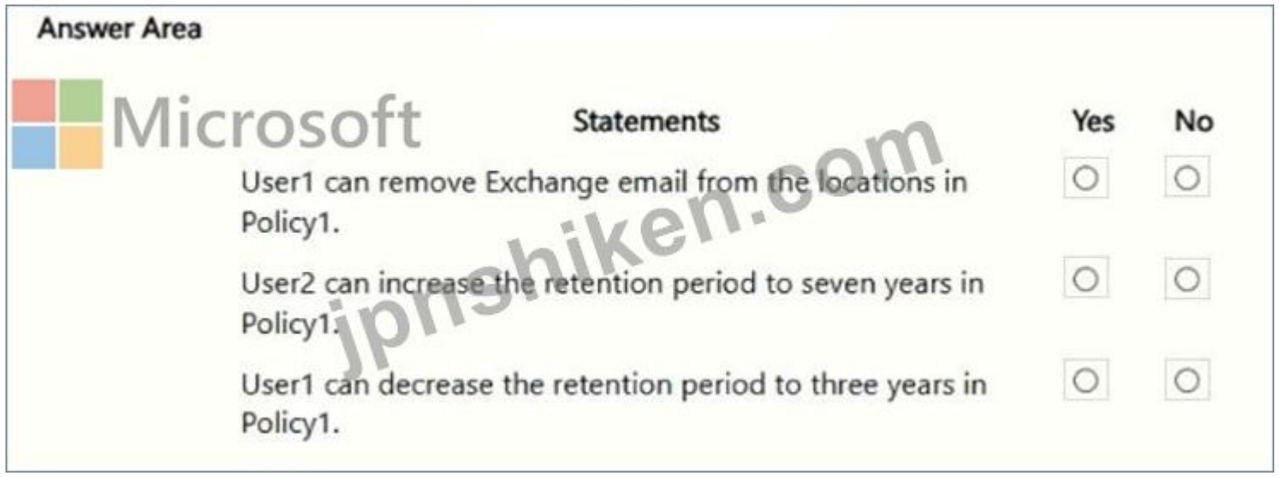
Explanation:
Box 1: No
File1 has two IP addresses in it.
Both Tip2 and Tip3 rules matches. Tip2 has higher priority.
Note: For the hosted service workloads, like Exchange Online, SharePoint Online and OneDrive for Business, each rule is assigned a priority in the order in which it's created. That means, the rule created first has first priority, the rule created second has second priority, and so on.
When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced.
Box 2: Yes
File2 has six IP addresses in it.
Only Rule3 matches.
Box 3: Yes
File3 has four IP addresses in it.
Both Rule2 and Rule3 matches.
Rule2 has higher priority.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference

質問**: 58**
ホットスポットに関する質問
次の表に示すユーザーを含む Microsoft 365 E5 テナントがあります。

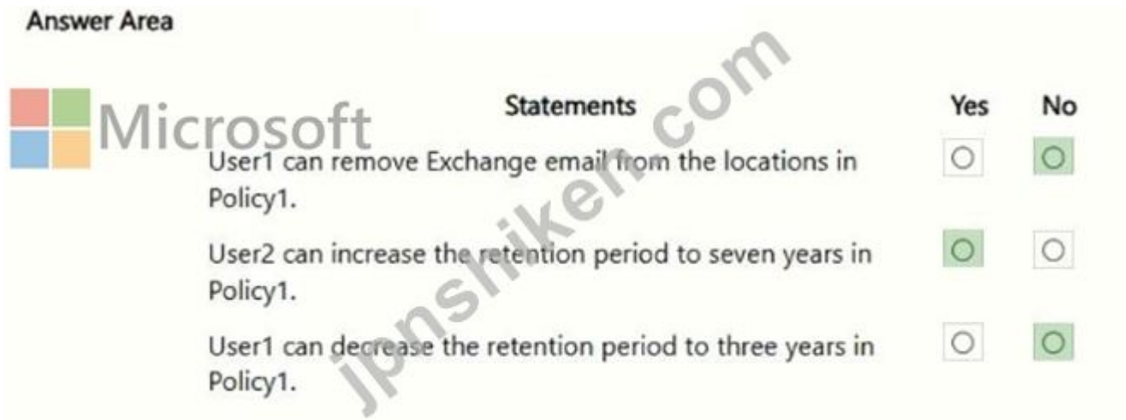
Name	Role
User1	Global Administrator
User2	Compliance Administrator

次のような構成の保持ポリシーがあります。
- アイテムを特定の期間保持する :5年間
- ポリシーを適用する場所: Exchange メール、SharePoint サイト
Policy1 に保存ロックを設定します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

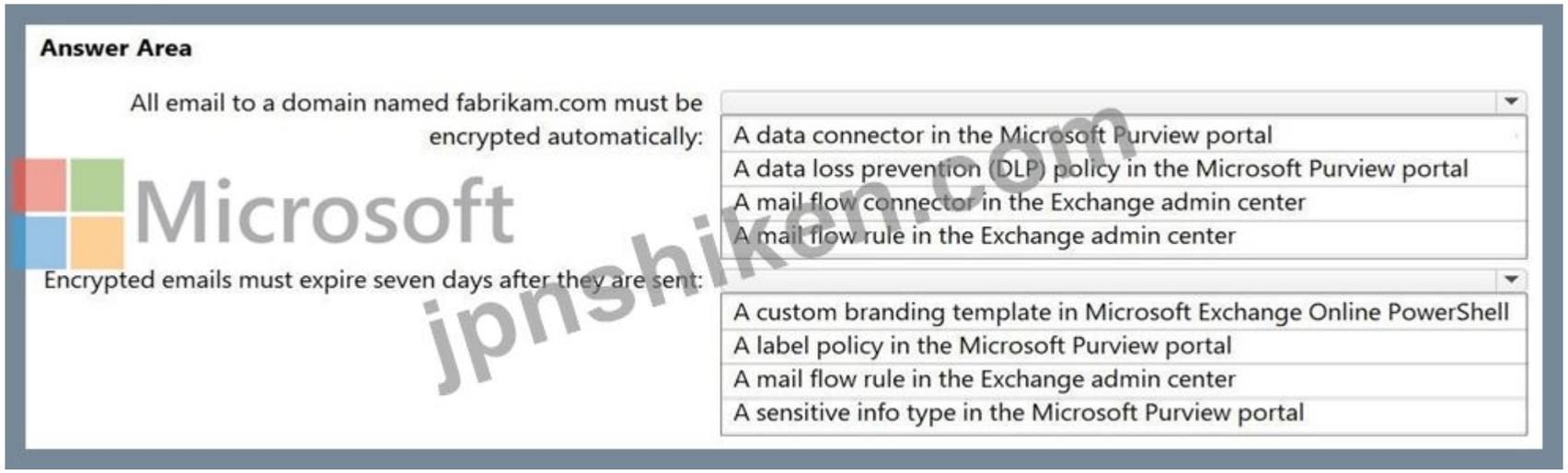


正解:

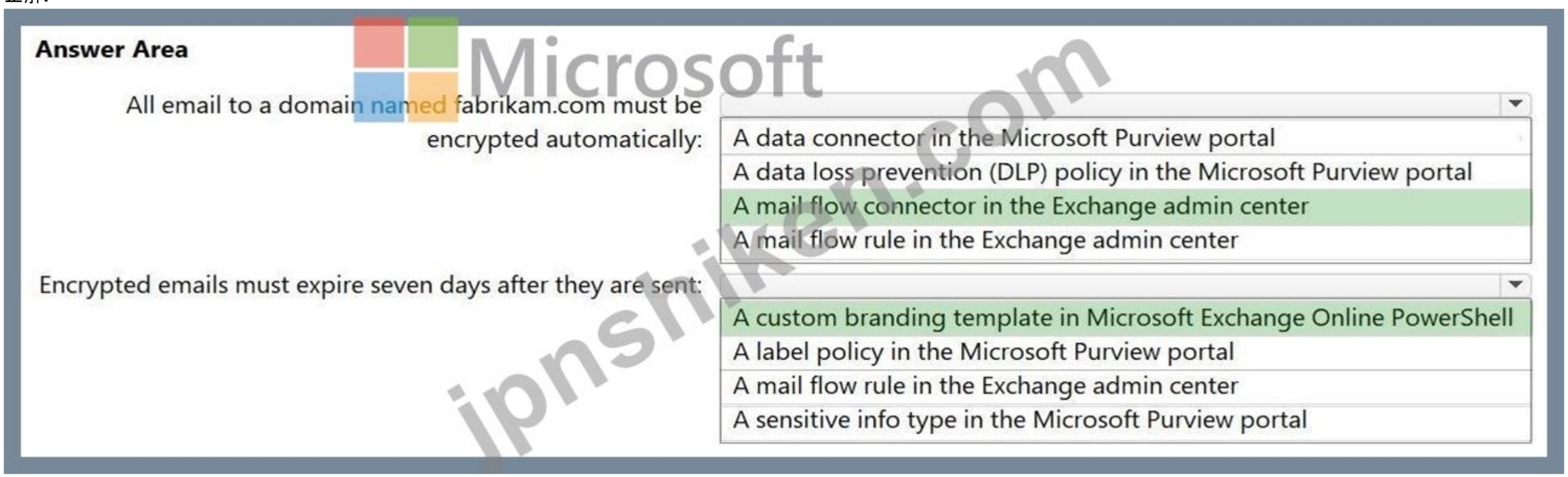


Explanation:
Box 1: No
When a retention policy is locked:
No one, including the global admin, can disable the policy or delete it Locations can be added but not removed You can extend the retention period but not decrease it Box 2: Yes You can extend the retention period but not decrease it Box 3: No You can extend the retention period but not decrease it Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock

質問: **59**
ホットスポットに関する質問
contoso.com という名前の Microsoft 365 テナントに Microsoft Purview Advanced Message Encryption を実装しています。
次の要件を満たす必要があります。
- fabrikam.comというドメイン宛のすべてのメールは暗号化する必要がある
自動的に。
- 暗号化された電子メールは送信後 7 日で期限切れになります。
各要件に対して何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

Box 1: A mail flow rule in Exchange admin center

To automatically encrypt all emails sent to a specific domain with Microsoft Purview Advanced Message Encryption, an administrator must first configure a sensitivity label with the desired encryption settings and then create an Exchange mail flow rule (also called a transport rule) in the Microsoft Purview portal to apply that sensitivity label to messages meeting the condition of being sent to the target domain.

Box 2: A custom branded template in Microsoft Exchange Online PowerShell You can use message expiration on emails that your users send to external recipients who use the OME Portal to access encrypted emails. You force recipients to use the OME portal to view and reply to encrypted emails sent by your organization by using a *custom branded template* that specifies an expiration date in PowerShell.

Reference:

https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage- mail-flow-rules

https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

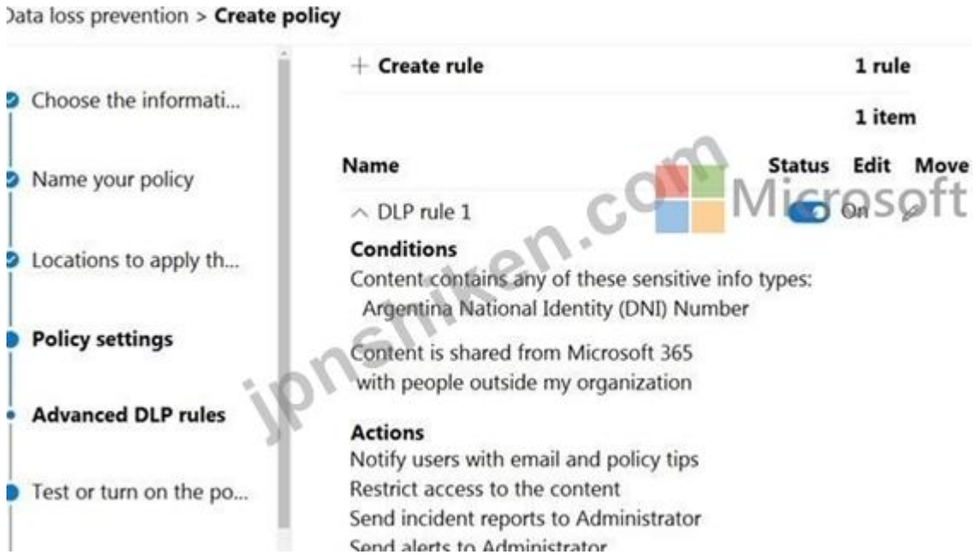
質問: **60**
Microsoft 365 E5 サブスクリプションをお持ちです。
個人情報 (PII) を含む会社のデータがサードパーティの生成 AI ツールと共有されるのを防ぐために、Microsoft Purview Data Security Posture Management for AI (OSPM for AI) を展開する予定です。
計画された展開の前提条件を完了する必要があります。
どの 2 つの Microsoft Purview ソリューションを使用する必要がありますか? それぞれの正解はソリューションの一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. データ損失防止
B. 情報障壁
C. インサイダーリスク管理
D. コミュニケーションコンプライアンス
E. 監査
正解: **(**正解を表示します**)**
[A] DLP helps protect confidential information such as financial records, personally identifiable information (PII), health data, or intellectual property by monitoring and controlling how this data is accessed, shared, or transmitted.
Organizations have sensitive information under their control, such as:
financial data
proprietary data
credit card numbers
health records
social security numbers
To help protect this sensitive data, and to reduce the risk from oversharing, they need a way to help prevent their users from inappropriately sharing sensitive data with people who shouldn't have it. This practice is called data loss prevention (DLP).
[D] Microsoft Purview Communication Compliance provides the tools to help organizations detect regulatory compliance (for example, SEC or FINRA) and business conduct violations such as sensitive or confidential information, harassing or threatening language, and sharing of adult content. Communication Compliance is built with privacy by design. Usernames are pseudonymized by default, role-based access controls are built in, investigators are opted in by an admin, and audit logs are in place to help ensure user-level privacy.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
https://learn.microsoft.com/en-us/purview/communication-compliance

質問: **61**
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
サブスクリプション内のデータの潜在的な過剰共有を識別するために、カスタム データ評価スキャンの使用を評価しています。
データ評価が場所ごとにサポートできるアイテムの最大数はいくつですか?
A. 50.000
B. 100.000
C. 200.000
D. 500.000
正解: **C (**コメントを発表する**)**

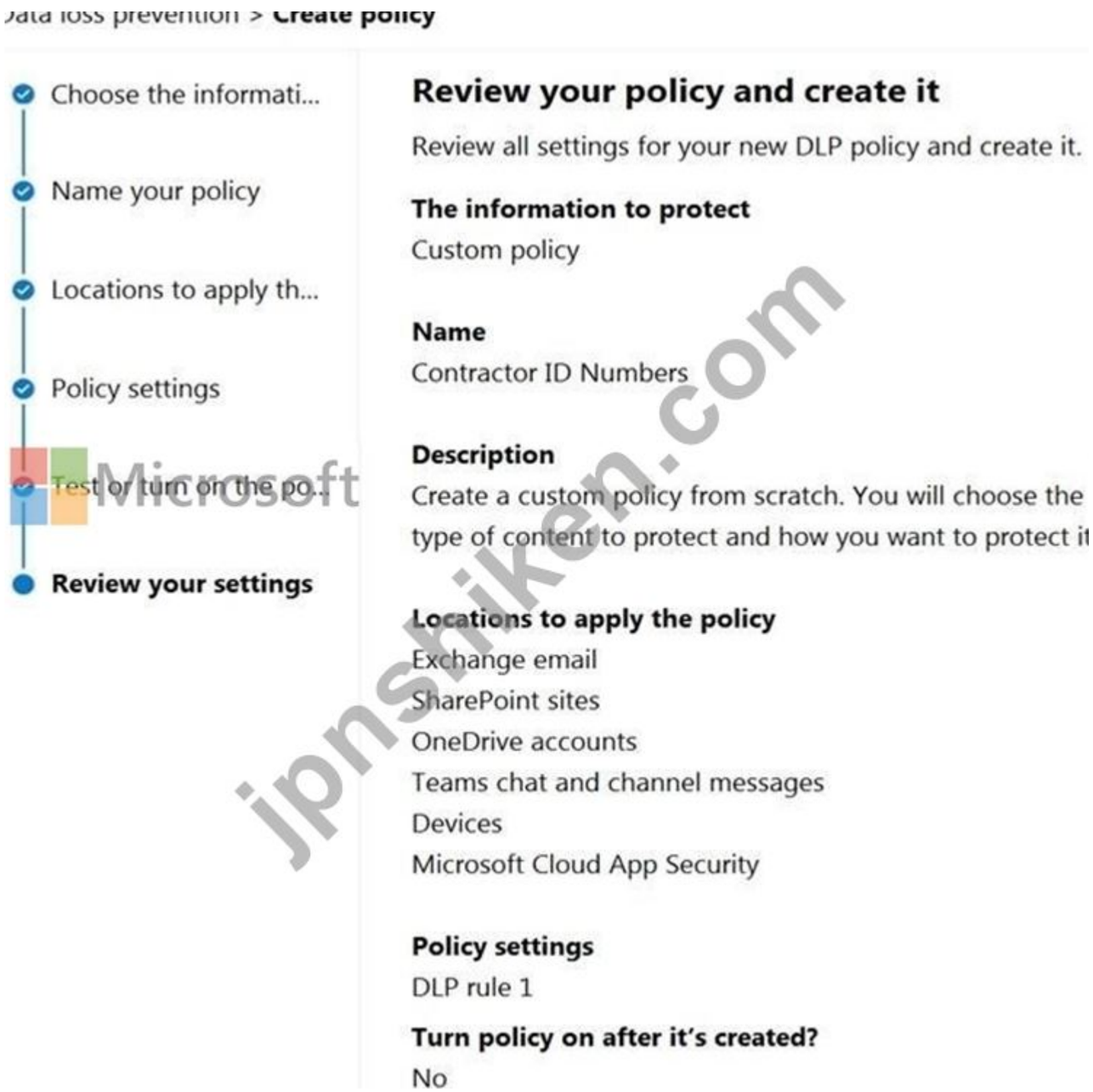
Data risk assessments currently support a maximum of 200,000 items per location.
Reference:
https://learn.microsoft.com/en-us/purview/dspm-for-ai

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
データ損失防止(DLP)ポリシーを作成します。 『ルール」パネルに 高度なDLPルール」ページが表示されます。(『ルール」タブをクリックします)



[設定の確認] ページが [レビュー] 展示内に表示されます。([レビュー] タブをクリックします。)



アクションを適用せずにポリシーを有効にした場合の潜在的な影響を確認する必要があります。
何をすべきでしょうか?

A. ポリシーを終了し、「まずテストしてみます」を選択します。

B. ポリシーを編集し、DLP ルール 1 のすべてのアクションを削除して、「まずテストしてみたい」を選択します。

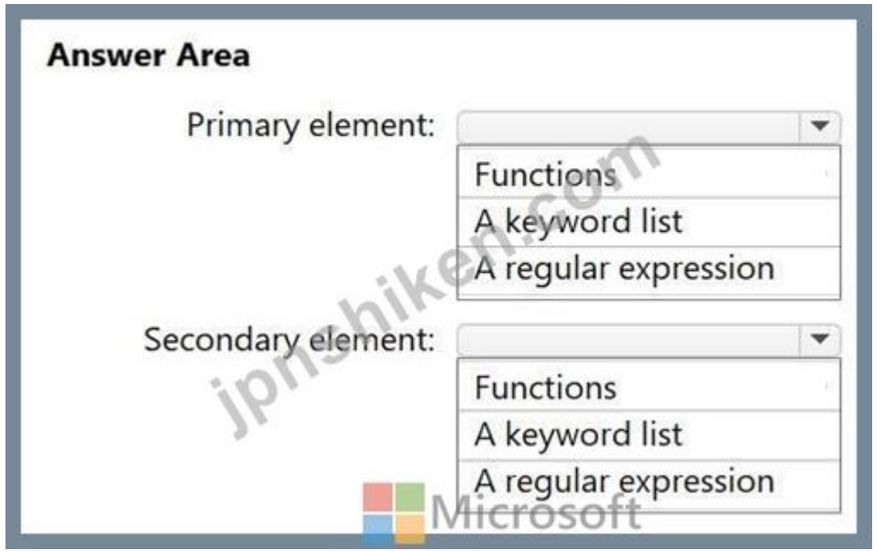
C. ポリシーを編集し、「コンテンツへのアクセスを制限する」および「インシデント レポートを管理者に送信する」アクションを削除して、「はい、すぐに有効にします」を選択します。

D. ポリシーを編集し、DLP ルール 1 のすべてのアクションを削除して、[はい、すぐにオンにします] を選択します。

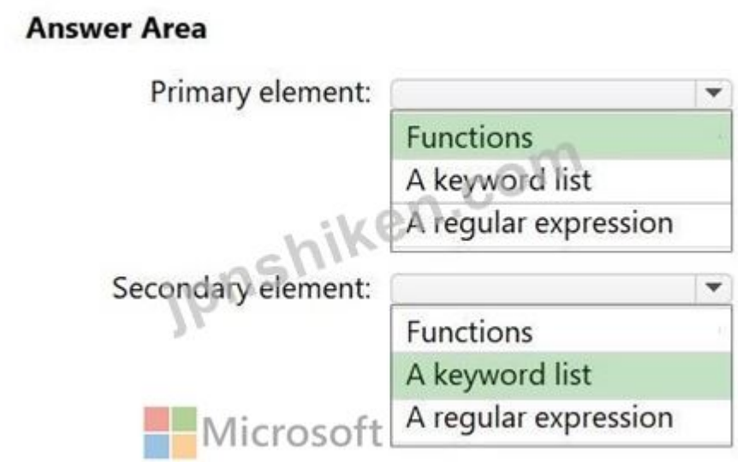
正解: **(**正解を表示します**)**

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template

質問: **63**
ホットスポットに関する質問
Microsoft 365 テナントがあります。
次の内容を含むアイテムに対して、新しい機密情報の種類を作成する必要があります。
- 従業員の雇用日を表す従業員ID番号
3桁の数字が続く
- 従業員 ID 番号の 300 文字以内に 「従業員」、「ID」、または 「識別」という単語 プライマリ要素とセカンダリ要素には何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:
Box 1: Functions
Need to include use a date function for the primary element.
Note: Create custom sensitive information types
The primary element can be a Regular expression with an optional validator, a Keyword list, a Keyword dictionary, or one of the pre-configured Functions.
Box 2: A keyword list

Use a keyword list which includes the words "Employee", "ID", or "Identification".
Reference:
https://learn.microsoft.com/en-us/purview/sit-learn-about-exact-data-match-based-sits

質問: **64**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com" を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク2
件名に "Falcon"という単語が含まれる外部受信者に送信される電子メールが、"Highly Confidential \ All Employees"という名前の RMS テンプレートを使用して暗号化されるようにする必要があります。
正解:
To encrypt emails with "Falcon" in the subject to external recipients, you must first create an Information Protection sensitivity label with RMS encryption, then create a mail flow rule in the Purview compliance portal that applies this label to emails that are sent externally and have
"Falcon" in the subject line.
Task 1: Set up the Information Protection sensitivity label
Step 1: Go to the Microsoft Purview compliance portal and navigate to Information protection.
Step 2: Open the Labels tab and click Create a label.
Step 3: Follow the wizard to configure the new label. On the label settings page, enable Encrypt and then select the RMS template that you want to apply.
Task 2: Create the mail flow rule
Step 4: Go to the Purview compliance portal and navigate to Mail flow rules.
Step 5: Click New rule.
Step 6: Set the conditions:
Condition 1: Select "The subject contains..." and enter "Falcon".
Condition 2: Select "The recipient is located..." and choose "External".
Step 7: Set the action:
Select "Apply the sensitivity label..." and choose the label you created in the previous step.
Step 8: Review and save the rule.
Reference:
https://learn.microsoft.com/en-us/purview/ome

質問: **65**
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
EDM1 という名前の完全データー致 (EDM) 分類子を作成しています。
EDM1 の場合、次の表に示すフィールドを含むスキーマ ファイルをアップロードします。

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

EDM1 が持つことができる主要要素の最大数はいくつですか?
A. 1
B. 2
C. 3
D. 4
正解: **(正解を表示します)**
In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.
From the provided table, the Match mode indicates how data is analyzed:
- PP (EU Passport Number) Likely a primary element because it's unique.
- Name (All Full Names) Typically not a primary element as names are common.
- DateOfBirth (Single-token) Usually a secondary element, not unique.
- AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.
- Since EDM supports a maximum of two primary elements, the correct answer is 2.

質問: **66**
社内でMicrosoft Purview Advanced Message Encryptionの機能をテストする必要があります。テストでは、以下の情報を確認する必要があります。
* 取得したデフォルトのテンプレート名
* 暗号化と復号化の検証ステータス
どの PowerShell コマンドレットを実行する必要がありますか?
A. テスト-OAuth接続

B. テスト-ClientAccessRule
C. テスト-IRMConfiguration
D. テストメールフロー
正解: (正解を表示します)
Verify Microsoft Purview Message Encryption configuration in Exchange Online PowerShell You can verify that your Microsoft 365 tenant is properly configured to use Microsoft Purview Message Encryption in Exchange Online PowerShell.
1. Using a work or school account that has sufficient permissions in your organization, such as Compliance Administrator, start a Windows PowerShell session and connect to Exchange Online.
For instructions, see Connect to Exchange Online PowerShell.
2. Run the Get-IRMConfiguration cmdlet.
You should see a value of $True for the AzureRMSLicensingEnabled parameter, which indicates that Microsoft Purview Message Encryption is configured in your tenant. If it is not, use Set-IRMConfiguration to set the value of AzureRMSLicensingEnabled to $True to enable Microsoft Purview Message Encryption.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities

質問: **67**
次の表に示すように、RP1 という名前のアイテム保持ポリシーが含まれる Microsoft 365 E5 サブスクリプションがあります。

Setting	Value
Location	• Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

RP1 に保存ロックをかけます。
RP1 を変更する必要があります。
どの 2 つの変更を実行できますか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. ポリシーに場所を追加します。
B. ポリシーを削除します。
C. ポリシーから場所を削除します。
D. ポリシーの保持期間を短縮します。
E. ポリシーを無効にします。
F. ポリシーの保持期間を延長します。
正解: (正解を表示します)
A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.
When a Preservation Lock is applied:
1. You cannot disable or delete the policy.
2. You cannot remove locations from the policy.
3. You cannot decrease the retention period.
4. You can add locations to the policy.
5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

質問: 68
ホットスポットに関する質問
次の図に示すように、Microsoft Entra テナント内のすべてのユーザーに公開されている Microsoft 365 機密ラベルがあります。

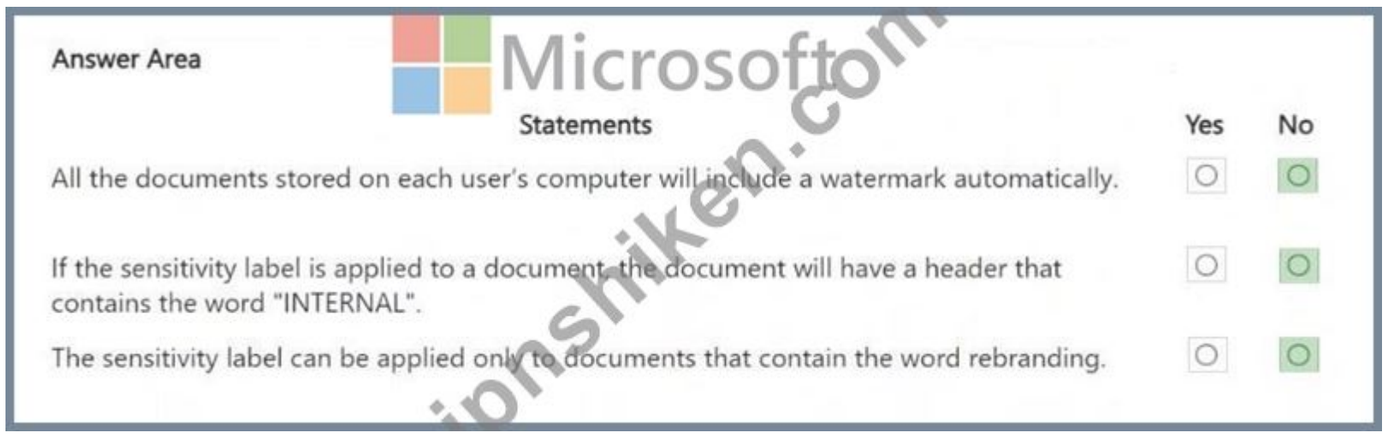


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

正解:



Explanation:
Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.
Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.
Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

質問: **69**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
次の表に示す監査保持ポリシーを作成します。

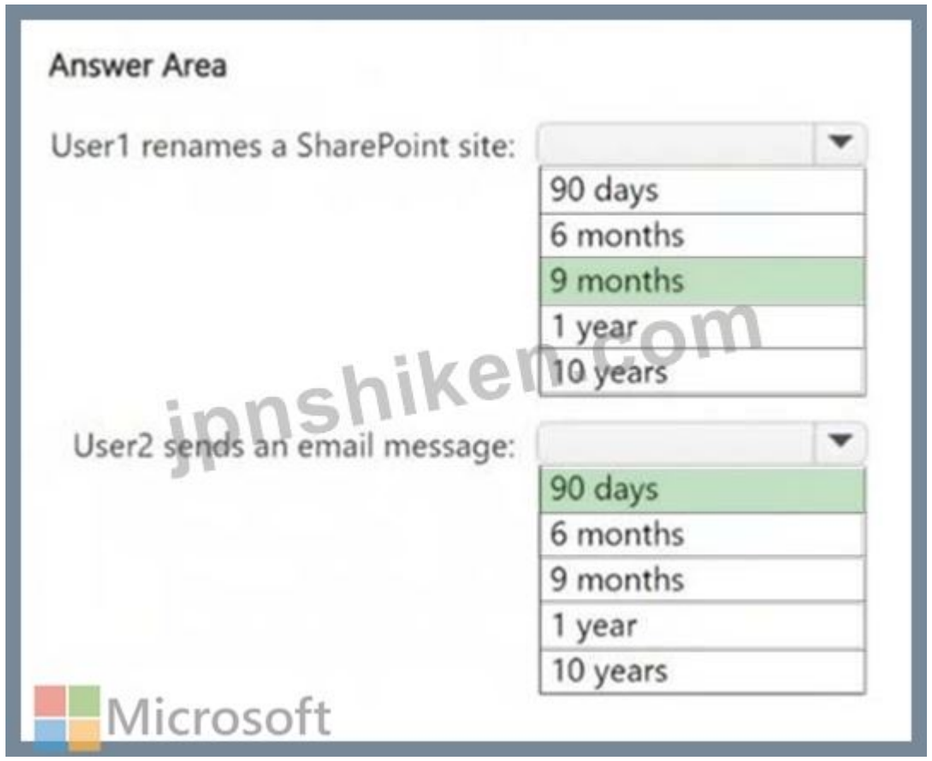
Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	*None*	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	*None*	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	*None*	10 Years

ユーザーは次のアクションを実行します。
- ユーザー1 が Microsoft SharePoint Online サイトの名前を変更します。
- ユーザー2が電子メールメッセージを送信します。

各アクションの監査ログ レコードはどのくらいの期間保持されますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

The action "SiteRenamed" for SharePoint is covered under the AuditRetention4 policy, which applies to User1 and retains logs for 9 months.

The action "Send" for ExchangeItem is covered under the AuditRetention2 policy, but this policy applies only to User1. Since User2 is not covered under a specific policy, the default retention period for audit logs in Microsoft Purview is 90 days.

質問**: 70**

ホットスポットに関する質問

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザーがChatGPTおよびGoogle Geminiに機密データをアップロードできないようにする必要があります。ソリューションは以下の要件を満たす必要があります。

- クレジットカード番号がChatGPTに貼り付けられるのを防ぎ、

ジェミニ。

- 機密データを含む文書が ChatGPT および Gemini にアップロードされないようにします。

各要件にはどの Microsoft Purview ソリューションを使用する必要がありますか? 回答するには、回答で適切なオプションを選択してください。注: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:

Answer Area



Explanation:

Box 1: Data Loss Prevention

Prevent credit card numbers from being pasted into ChatGPT and Gemini.

Microsoft Purview data security and compliance protections for generative AI apps The Data Loss Prevention Policy (DLP) serves as a safeguard against sensitive data being copied, pasted, or uploaded into external AI platforms.

Windows computers that are onboarded to Microsoft Purview can be configured for Endpoint data loss prevention (DLP) policies that warn or block users from sharing sensitive information with third-party generative AI sites that are accessed via a browser. For example, a user is prevented from pasting credit card numbers into ChatGPT, or they see a warning that they can override.

Box 2: Data Loss Prevention

Prevent documents that contain classified data from being uploaded to ChatGPT and Gemini.

Data Loss Prevention (DLP) Policy: Preventing Sensitive Data from Being Shared The Data Loss Prevention Policy (DLP) serves as a safeguard against sensitive data being copied, pasted, or uploaded into external AI platforms. This policy ensures that any confidential, personal, or proprietary information is blocked from being transferred to unauthorized AI websites like ChatGPT or Google Gemini.

Reference:

https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

質問: 71

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 エンドポイントのデータ損失防止 (エンドポイント DLP) を実装します。
Windows 11 を実行し、Microsoft 365 アプリがインストールされたコンピューターがあります。これらのコンピューターは Microsoft Entra テナントに参加しています。
エンドポイント DLP ポリシーがコンピューター上のコンテンツを保護できることを確認する必要があります。
解決策: コンピューターを Microsoft Intune に登録します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解**: (**正解を表示します**)**
Correct:
* You deploy the Endpoint DLP configuration package to the computers.
* You onboard the computers to Microsoft Defender for Endpoint.
Incorrect:
* You deploy the unified labeling client to the computers.
* You enroll the computers in Microsoft Intune.
* You deploy the Microsoft Purview Information Protection client to the computers.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints

質問**: 72**
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Purview Data Security Posture Management for AI (DPSM for AI) を展開します。
展開の一環として作成されたデフォルトポリシーを、User1 が確認できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 をどのロール グループに追加する必要がありますか?
A. コンプライアンス管理者およびコンプライアンスデータ管理者
B. Microsoft Exchange Online のコンテンツ エクスプローラー コンテンツ ビューアーと表示専用組織管理
C. セキュリティリーダーおよびインサイダーリスク管理調査員
D. Microsoft Exchange Online のコンプライアンス管理と組織管理
正解**: C (**コメントを発表する**)**
Microsoft Purview Security Reader role group and also Insider Risk Management Investigators.
Note:
Permissions for Data Security Posture Management for AI
Members of your security and compliance teams who are responsible for managing AI apps in the Microsoft Purview Data Security Posture Management for AI need appropriate permissions when they sign in to the Microsoft Purview portal.
Permissions by activities

Activities	Microsoft Entra Compliance Administrator role	Microsoft Entra Global Administrator role	Microsoft Purview Compliance Administrator role group	Roles or role groups that are view-only*	When not supported, additional role groups required
View all policies in the policy list	✓	✓	✓	✓ Excludes: Insider risk management policies Communication compliance policies	For insider risk management polices: Microsoft Purview Insider Risk Management Administrator Microsoft Purview Insider Risk Management Analyst Microsoft Purview Insider Risk Management Investigator

Microsoft
jpnshiken.com

Note 2:
Roles and role groups that can view, create, and edit in Data Security Posture Management for AI:
Microsoft Entra Compliance Administrator role
Microsoft Entra Global Administrator role
Microsoft Purview Compliance Administrator role group
Roles and role groups that can view-only in Data Security Posture Management for AI:
*-> Microsoft Purview Security Reader role group
Purview Data Security AI Viewer role
AI Administrator role from Entra
Purview Data Security AI Content Viewer role for AI interactions only
Purview Data Security Content Explorer Content Viewer role for AI interactions and file details for data risk assessments only Reference:
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-permissions

質問**: 73**
次の表に示すような Microsoft 365 E5 テナントと Windows クライアント デバイスがあります。

Name	Joined to Microsoft Entra	Configuration
Device1	Yes	Onboarded to Microsoft Purview
Device2	Yes	Onboarded to Microsoft Defender for Endpoint
Device3	Yes	Enrolled in Microsoft Intune
Device4	No	Enrolled in Microsoft Intune

Microsoft 365 エンドポイント データ損失防止 (エンドポイント DLP) 設定はどのデバイスに適用できますか?

A. デバイス1のみ

B. デバイス1とデバイス2のみ

C. デバイス1とデバイス3のみ

D. デバイス1、デバイス3、デバイス4のみ

E. デバイス1、デバイス2、デバイス3、およびデバイス4

正解: **(**正解を表示します**)**

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started

質問: **74**

Site1 という名前の Microsoft SharePoint Online サイトと、次の表に示すデータ損失防止 (DLP) ポリシーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

DLP ルールは次の表のように構成されます。

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

すべてのポリシーは Site1 に割り当てられます。

ユーザーがすべてのルールに一致するドキュメントを Site1 にアップロードした場合、ユーザーに Tip 2 ポリシー ヒントが表示されるようにする必要があります。

何をすべきでしょうか?

A. Rule1 に一致する場合、ポリシーの追加処理を有効にします。

B. Rule2 に一致する場合、ポリシーの追加処理を防止します。

C. DLP2 の優先度を 3 に変更します。

D. DLP2 の優先度を 0 に変更します。

正解: **(**正解を表示します**)**

The rule with priority 0 is processed first.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference

質問: **75**
ホットスポットに関する質問
次の表に示すデバイス構成を含む Microsoft 365 E5 サブスクリプションがあります。

Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

各構成では、Google Chrome または Firefox のいずれかをデフォルトのブラウザとして使用します。
Microsoft Purview を実装し、構成に Microsoft Purview ブラウザ拡張機能を展開する必要があります。
各拡張機能はどの構成にデプロイできますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Google Chrome:
- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

Firefox:
- Config1 only
- Config2 only
- Config1 and Config2 only
- Config2 and Config3 only
- Config1, Config2, and Config3

正解:



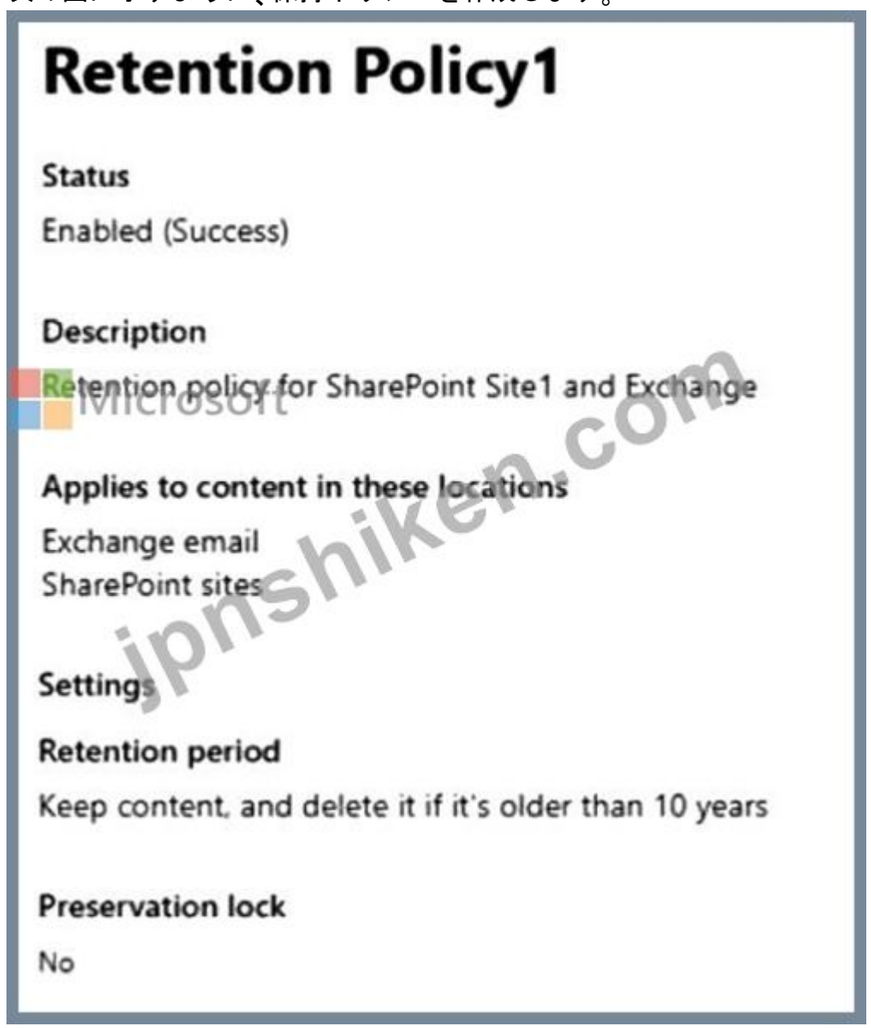
Explanation:
Microsoft Purview browser extensions for Endpoint DLP are supported on:
- Windows 10/11 (Config1)
- macOS (Config2)
- Not supported on Android (Config3)
Since Microsoft Purview does not support browser extensions on Android, Config3 is excluded from both Google Chrome and Firefox.

質問: **76**
保持ラベル ポリシーを持つ Microsoft 365 テナントがあります。
次の要件を満たすようにポリシーを構成する必要があります。
- ポリシーの無効化または削除を防止します。
- 新しいラベルを追加できることを確認します。
- ラベルの削除を防止します。
何をすべきでしょうか?
A. インサイダーリスク管理を有効にします。
B. 規制記録オプションを有効にします。
C. ファイル プランをインポートします。
D. 保存ロックを作成します。
正解: **(**正解を表示します**)**
A Microsoft 365 preservation lock on a retention label policy protects it from being disabled, deleted, or made less restrictive, and also prevents the removal of labels. This action makes the policy irreversible and is typically used to meet regulatory compliance requirements. Once locked, the policy can only be made more restrictive (e.g., by extending the retention period), but not less so.

How a preservation lock affects a retention policy
* Disabling and Deleting: No one, including global administrators, can turn off or delete the policy once it's locked.
* Removing Labels: Once a label is applied, it cannot be removed from a locked policy, nor can content be removed during the retention period.
* Etc.
Reference:
https://learn.microsoft.com/en-us/purview/retention

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 77
ホットスポットに関する質問
次の図に示すように、保持ポリシーを作成します。



User1 というユーザーが、Site1 という Microsoft SharePoint Online サイトから File1.docx というファイルを削除します。
User2 というユーザーが電子メールを削除し、Microsoft Outlook の削除済みアイテム フォルダーを空にします。
削除後 1 年間コンテンツはどこに保存されますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:

Answer Area



Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

質問: 78

Microsoft 365 E5 サブスクリプションがあり、User1、User2、User3、User4 という 4 人のユーザーと、File1.docx というファイルが含まれています。File1 には機密ラベルが適用されています。ラベルは、次の表に示すように構成されています。

User	Permission
User1	Owner
User2	Editor
User3	Restricted Editor
User4	Viewer

Microsoft 365 Copilot を使用して File1 を要約できるのはどのユーザーですか?

A. ユーザー1のみ

B. ユーザー1とユーザー2のみ

C. User1、User2、User3のみ

D. ユーザー1、ユーザー2、ユーザー3、ユーザー4

正解: **(**正解を表示します**)**

To summarize a file with a sensitivity label using Microsoft 365 Copilot, a user needs the EXTRACT and VIEW usage rights, especially if the sensitivity label applies encryption, according to Microsoft Learn. These rights are necessary for Copilot to access and process the content of the file, according to Microsoft Learn. If the user doesn't have these rights, Copilot won't be able to summarize the file.

* User1 - Yes

An owner has EXTRACT and VIEW usage rights.

* User2 - Yes

A user with Editor permissions can summarize a file with a sensitivity label using Microsoft 365 Copilot, but only if the sensitivity label grants the necessary usage rights, specifically the "EXTRACT" right, to the user. If the sensitivity label restricts the "EXTRACT" right, Copilot will not be able to summarize the file.

* User3 - No

A Restricted Editor in Microsoft 365 Copilot cannot summarize a file with a sensitivity label that restricts access. Microsoft 365 Copilot respects sensitivity labels and will not process files if the user doesn't have the necessary permissions (like EXTRACT and VIEW). If a user only has VIEW rights, Copilot will provide a reference link to the file instead of summarizing it.

* User4 - No

Reference:

https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data- protection-auditing

質問**: 79**

ホットスポットに関する質問

完全データー致 (EDM) を使用するカスタムの機密情報の種類を作成する予定です。

Microsoft 365 にアップロードするものと、アップロードに使用するツールを特定する必要があります。

何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。

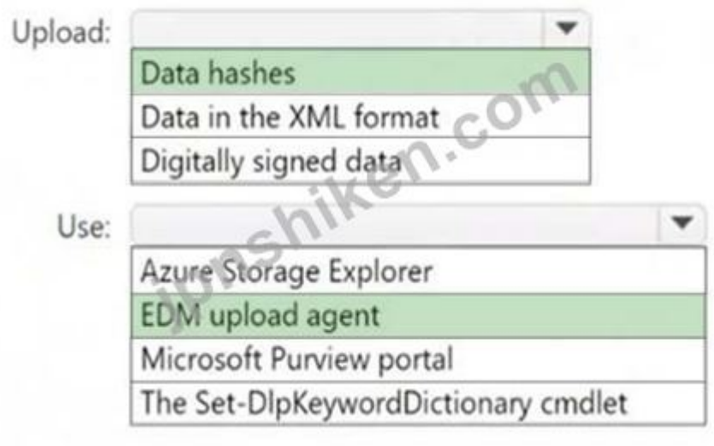
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:

Answer Area



Explanation:
EDM Upload Agent creates hashes for your SITs and saves them in the .CSV format. However you can also upload .csv, .tsv or pipe (|) formatted files. It also saves schema in XML format.

質問: **80**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX

Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL 「https://admin microsoft.com」を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク4
PCIデータセキュリティ基準(PCI DSS)の対象となる情報を含むメールの送信をユーザーからブロックする必要があります。このソリューションはメールのみに適用する必要があります。
正解**:**
Note: Policy templates
DLP policy templates are sorted into four categories:
* policies that can detect and protect types of Financial information.
Includes PCI Data Security Standard (PCI DSS), Credit card number
* Medical and health
* Privacy
* Custom policy
Use the EAC to configure a DLP policy from a template
Step 1: In the EAC, navigate to Compliance management > Data loss prevention, and then click Add Add Icon.
Step 2: On the Create a new DLP policy from a template page, complete the following fields:
Step 3: Name: Add a name that will distinguish this policy from others.
Step 4: Description: Add an optional description that summarizes this policy.
Step 5: Choose a template: Select the appropriate template to begin creating a new policy.
Step 6: Select the Payment Card Industry Data Security Standard (PCI DSS) template.
Step 7: More options: Select the mode or state. The new policy is not fully enabled until you specify that it should be. The default mode for a policy is test without notifications.
Step 8: Click Save to finish creating the policy.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-policy-reference
https://learn.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/create- dlp-policy-from-template

質問**: 81**
Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、Microsoft Purview にオンボードされたデバイスが 500 台含まれています。
Microsoft Purview Audit のアクティブ化を選択します。
ユーザーと生成 AI ウェブサイト間のやり取りを追跡できることを確認する必要があります。
デバイスに何を展開する必要がありますか?
A. Microsoft Purview拡張機能
B. Microsoft Purview Information Protection クライアント
C. Microsoft Defender ブラウザ保護拡張機能
D. エンドポイント分析
正解**: (**正解を表示します**)**
To track interactions between users and generative AI websites in Microsoft Purview Audit, you need to deploy the Microsoft Purview browser extension to the devices. This extension enables tracking of user activities on web-based applications, including AI-related tools like ChatGPT, Microsoft Copilot, and other generative AI platforms.

Microsoft Purview extension provides visibility into browser-based activities, including AI tool usage, ensuring compliance and risk management within Microsoft Purview. This extension works with Microsoft Edge and Google Chrome to track and log user interactions.

質問: **82**
ホットスポットに関する質問
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
次の要件を満たす電子メール メッセージのコンテンツ検索を実行する必要があります。
- user1@contoso.com と user2@contoso.com の両方に配信されます
- 名前が
コンプライアンスという言葉
KQL エディターでクエリを完了するにはどうすればよいでしょうか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

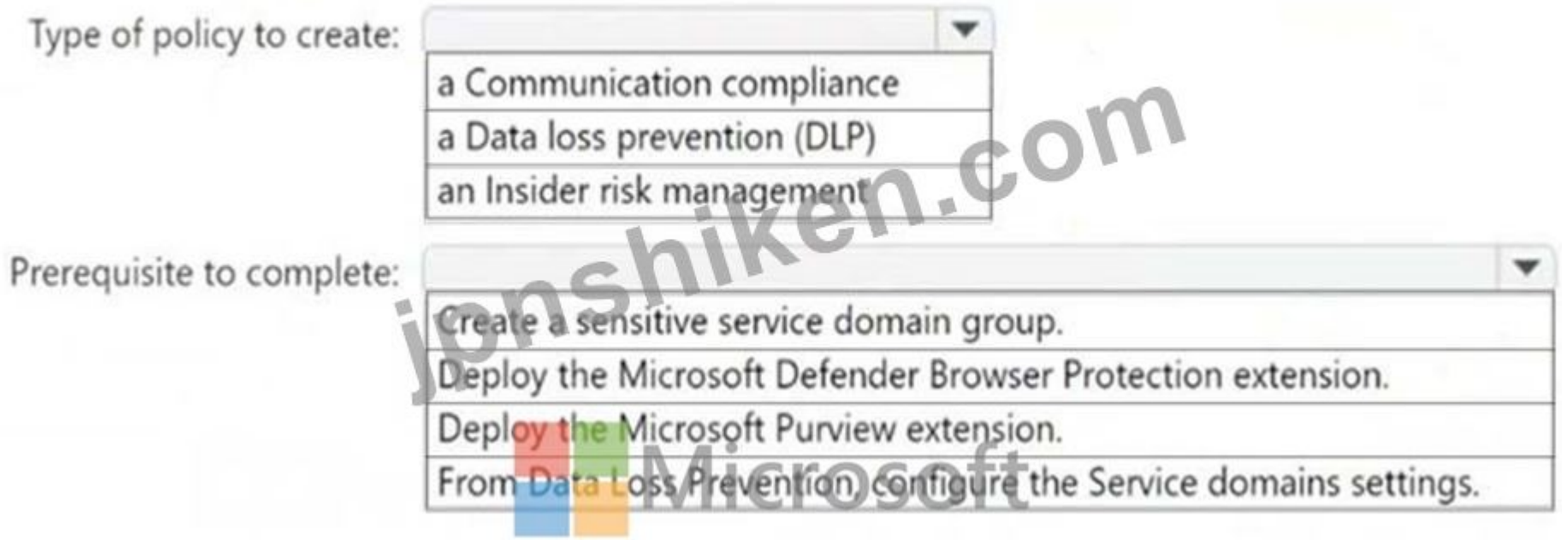


Explanation:
Box 1: "User1@contoso.com AND User2@contoso.com"
Delivered to both, so we must use AND.
Note:
A space between two keywords or two property:value expressions is the same as using OR. For example, from:"Sara Davis" subject:reorganization returns all messages sent by Sara Davis or messages that contain the word reorganization in the subject line.
Box 2: "Compliance*"
Reference:
https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

質問: **83**
Microsoft 365 E5 サブスクリプションをお持ちです。
Label1という機密ラベルを作成する必要があります。このソリューションでは、ユーザーがMicrosoft 365 Copilot を使用して、Label1 が適用されたファイルを要約します。
Label1 にはどの権限を選択する必要がありますか?
A. コンテンツのエクスポート(EXPORT)
B. コンテンツをコピーして抽出する(EXTRACT)
C. コンテンツの編集(DOCEDIT)
D. 表示権限(VIEW)
正解: **(正解を表示します)**
If content grants a user VIEW usage rights but not EXTRACT:
Copilot won't summarize this content but can reference it with a link so the user can then open and view the content outside Copilot.
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview-considerations

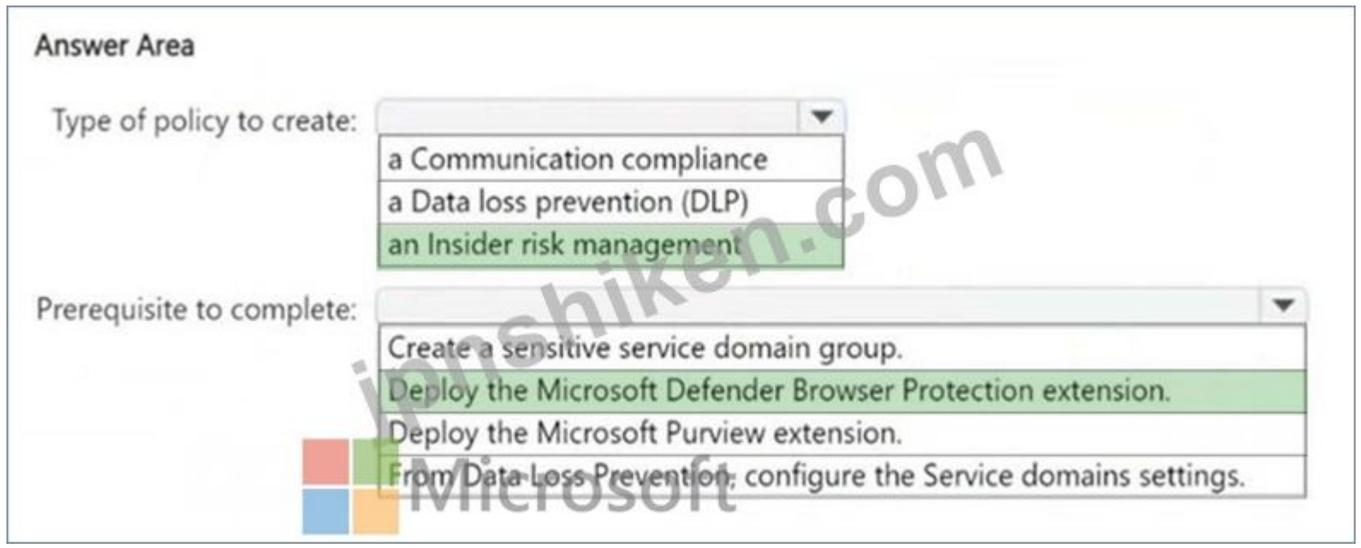
質問: **84**
ホットスポットに関する質問
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
ユーザーがフィッシング Web サイトにアクセスしたときにインシデントが生成されるようにする必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



jpnshiken.com
Microsoft

正解:



Explanation:

Box 1: Insider Risk Management policies in Microsoft Purview can be configured to detect risky behavior, such as accessing phishing websites. These policies monitor user activity, generate alerts, and help organizations investigate potential security threats.

Box 2: Microsoft Defender Browser Protection extension helps in detecting unsafe or phishing websites and integrating this detection with Insider Risk Management policies. This extension works with Microsoft Edge and Google Chrome to identify risky browsing activity and trigger alerts.

質問: 85

Microsoft 365 E5 サブスクリプションがあり、そこには Channel1 という Microsoft Teams チャネルが含まれています。Channel1 には研究開発ドキュメントが含まれています。

サブスクリプションに Microsoft 365 Copilot を実装する予定です。

Channel1 に保存されているファイルの内容が、Copilot によって生成された回答に含まれて、権限のないユーザーに表示されるのを防ぐ必要があります。

何を使うべきでしょうか?

A. 機密ラベル

B. コミュニケーションコンプライアンスポリシー

C. Microsoft Purview インサイダーリスク管理

D. Microsoft Purview 情報バリア (IB)

正解: (正解を表示します)

Correct:

* sensitivity labels

To prevent the contents of files stored in Channel1 from being included in Microsoft 365 Copilot responses and ensure unauthorized users cannot access them, you should use Microsoft Purview Sensitivity Labels.

Sensitivity labels allow you to classify, protect, and restrict access to sensitive files. You can configure label-based encryption and access control policies to ensure that only authorized users can access or interact with the files in Channel1. Microsoft 365 Copilot respects sensitivity labels, meaning if a file is labeled with restricted permissions, Copilot will not use it in generated responses for unauthorized users.

Incorrect:

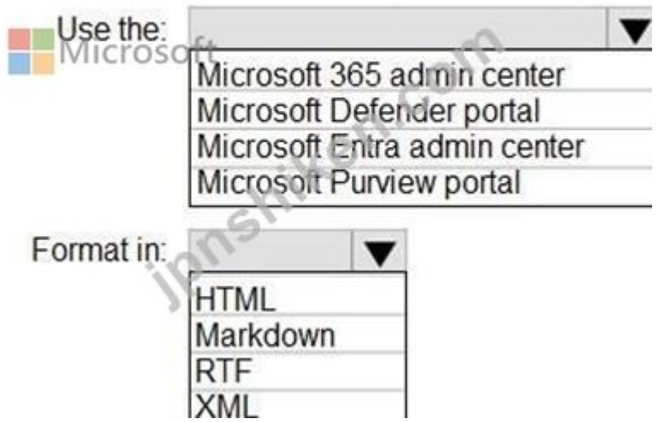
* communication compliance policy
* data loss prevention (DLP)
* Microsoft Purview Information Barriers (IBs)

* Microsoft Purview insider risk management
Note:
To prevent unauthorized access to channel file contents via Microsoft 365 Copilot, apply sensitivity labels with Data Loss Prevention (DLP) policies to restrict content processing. Additionally, manage channel memberships, restrict sharing links in SharePoint, and enforce external access policies.
Use sensitivity labels and DLP policies
1. Apply labels: Assign sensitivity labels like "Confidential" to sensitive documents in the channel.
2. Create DLP policies: In Microsoft Purview, configure a policy to prevent Copilot from processing content that has specific sensitivity labels. This stops Copilot from summarizing sensitive files for unauthorized users.
Reference:
https://learn.microsoft.com/en-us/purview/ai-m365-copilot-considerations

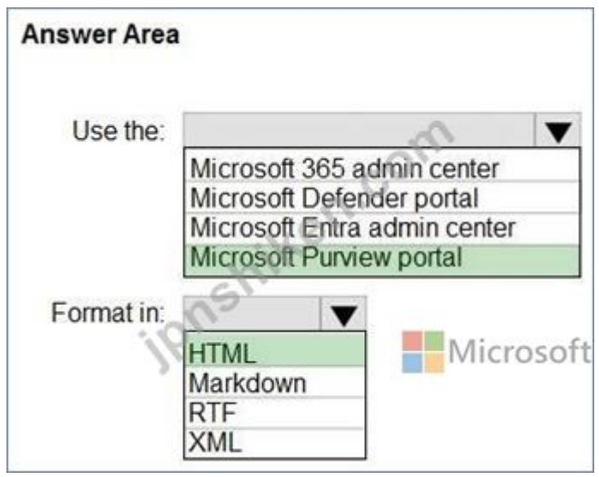
質問**: 86**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を使用する予定です。
辞職を申し出たユーザーや雇用終了日が近いユーザーによる Microsoft SharePoint Online からのデータ盗難を検出するインサイダー リスク管理ポリシーを作成する必要があります。
まず何をすべきでしょうか?
A. Office インジケーターを構成します。
B. HR データ コネクタを構成します。
C. 物理バッジコネクタを構成します。
D. デバイスを Microsoft Defender for Endpoint にオンボードします。
正解**: (**正解を表示します**)**
https://learn.microsoft.com/en-us/purview/import-hr-data?tabs=microsoft-purview-portal

質問**: 87**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。
インサイダーリスク管理を実装しています。
インサイダー リスク管理通知テンプレートを作成し、通知テンプレートのメッセージ本文をフォーマットする必要があります。
テンプレートをどのように構成すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



正解:



Explanation:

Box 1: Microsoft Purview portal

Create insider risk management notice templates

To create a new insider risk management notice template, you'll use the notice creation tool in Insider risk management solution in the Microsoft Purview portal.

Box 2: HTML

HTML for notices

If you'd like to create more than a simple text-based email message for notifications, you can create a more detailed message by using HTML in the message body field of a notice template.

Reference:

https://learn.microsoft.com/en-us/purview/insider-risk-management-notices

質問: **88**

ドラッグアンドドロップの質問

20 個のデータ損失防止 (DLP) ポリシーが含まれる Microsoft 365 サブスクリプションがあります。

次の点を特定する必要があります。

- ポリシーアラートをトリガーせずに適用されるルール
- DLPポリシーに一致した上位10個のファイル

- 誤って分類されたアラート
各要件にはどのレポートを使用すべきでしょうか？適切なレポートを適切な要件にドラッグしてください。各レポートは1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

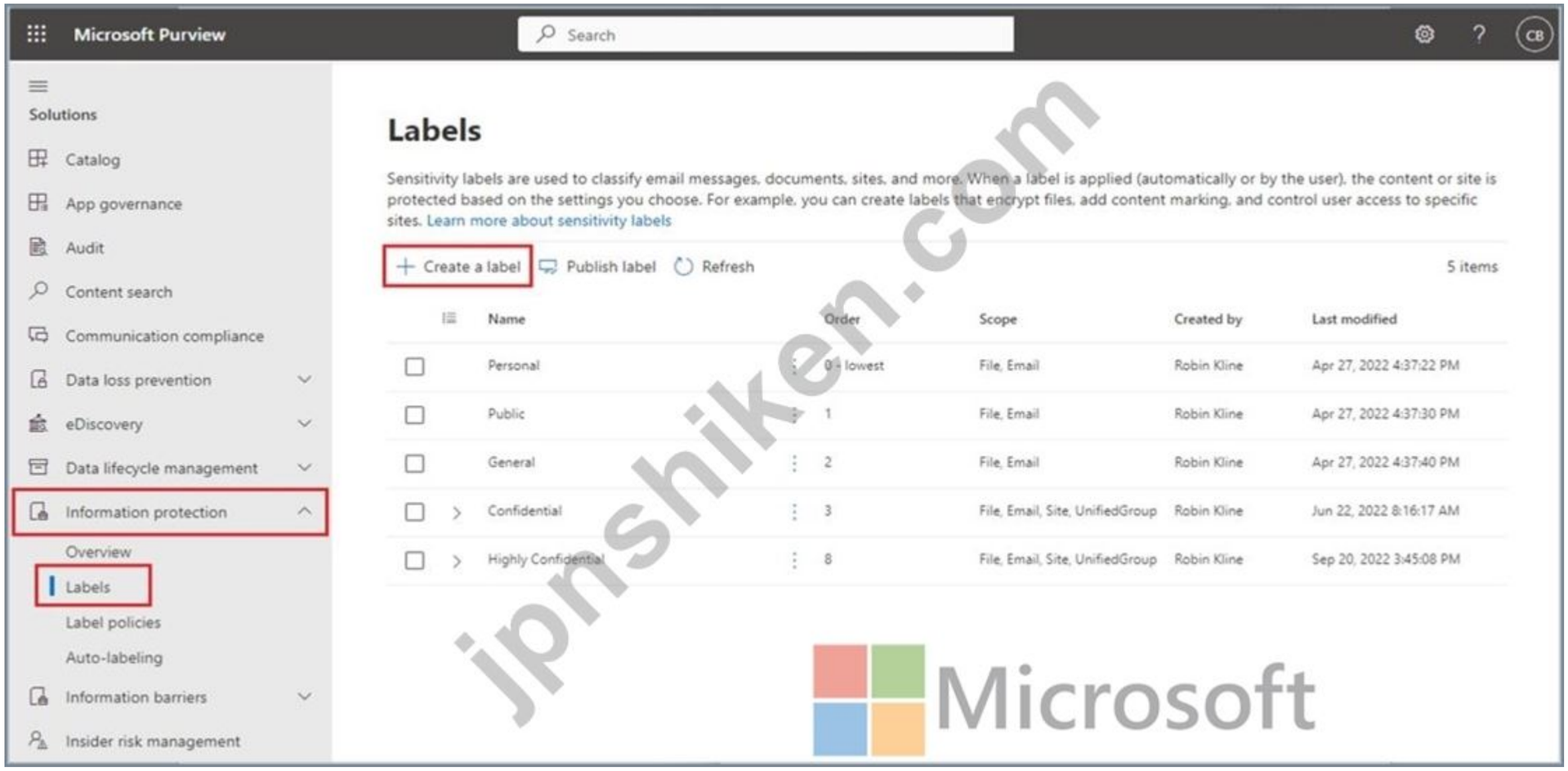


質問: **89**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
最近、会社の開発者が Azure ストレージ アカウント キーをプレーン テキストで第三者に電子メールで送信していることが分かりました。
Azure ストレージ アカウント キーを電子メールで送信する場合は、電子メールが暗号化されていることを確認する必要があります。
解決策: Exchange 電子メール、SharePoint サイト、OneDrive アカウント、Teams のチャットとチャネル メッセージが選択されたデータ損失防止 (DLP) ポリシーを作成します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **A** (コメントを発表する)
Correct:
* You create a data loss prevention (DLP) policy that has only the Exchange email location selected.
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

* You create a data loss prevention (DLP) policy that has Exchange email, SharePoint sites, OneDrive accounts, and Teams chat and channel messages selected.OneDrive accounts, and Teams chat and channel messages selected.
Creating a Data Loss Prevention (DLP) policy that includes Exchange email as a location can help detect and prevent the sharing of sensitive information, like Azure Storage keys, in plain text. By setting up a DLP policy with conditions to identify Azure Storage keys and enforce encryption or blocking actions for Exchange email, the policy will ensure that any emails containing such sensitive information are either encrypted or prevented from being sent.
Incorrect:
* You configure a mail flow rule that matches a sensitive info type.
* You configure a mail flow rule that matches the text patterns.
To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.
Text patterns in mail flow rules are not as reliable as sensitive information types in DLP.
Mail flow rules lack advanced content detection and machine learning-based classification, making them less effective than DLP.
* You create a data loss prevention (DLP) policy that has all locations selected.
Reference:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and- exceptions

質問**: 90**
ユーザーがMicrosoft OneDriveから社外のユーザーと機密文書を共有した場合、アラートを受け取る必要があります。どうすればよいでしょうか？
A. Microsoft Defender ポータルからファイル ポリシーを作成します。
B. Exchange 管理センターから、データ損失防止 (DLP) ポリシーを作成します。
C. Microsoft Entra 管理センターから、Identity Protection ポリシーを構成します。
D. Microsoft Defender ポータルからアクティビティ ポリシーを作成します。
正解**: (**正解を表示します**)**
Correct:
* From the Microsoft Defender portal, create an activity policy.
An activity policy in Microsoft Defender for Cloud Apps (Microsoft Defender portal) allows you to track and alert on specific user actions, such as sharing sensitive documents externally from OneDrive. This policy can detect file-sharing activities and send alerts when files are shared with external users, which meets the requirement.
Incorrect:
* From the Exchange admin center, create a data loss prevention (DLP) policy.
From the Exchange admin center you can only configure mail flow rules to detect sensitive info and apply actions like encryption or blocking, which are essentially DLP functions within Exchange.
* From the Microsoft Defender portal, create a file policy.
Is correct only if sensitive documents already have been shared.
* From the Microsoft Entra admin center, configure an Identity Protection policy.
* From the Microsoft Purview portal, create an insider risk policy.
* From the Microsoft Purview portal, start a data investigation.
* From the Microsoft Purview portal, start an Advanced eDiscovery search.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-create-policy-spo-odb-external

質問: **91**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク3
Falcon というプロジェクトのドキュメントに透かしを自動的に適用する予定です。
ドキュメントの斜めに、赤色でサイズ 12 のフォントで "Project Falcon"という透かしを追加するラベルを作成する必要があります。
正解:
Create and configure sensitivity labels
Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels Step 2: On the Labels page, select + Create a label to start the new sensitivity label configuration:



Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published.
In our case select: Items, Files, and select Word documents.



Note: If Items is selected, you can configure settings that apply to apps that support sensitivity labels, such as Office Word and Outlook. Optionally, you can extend these labels to include meetings from Teams and Outlook, and to protecting Teams meetings themselves by enforcing settings for Teams meetings and related chat.

Step 4: Follow the configuration prompts for the label settings. Use the help in the UI for individual settings.

Step 5: In the UI add a watermark of "Project Falcon" in red, size-12 font diagonally across the document.

Note: What sensitivity labels can do

After a sensitivity label is applied to an email, meeting invite, or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:

* Mark the content when you use Office apps, by adding watermarks, headers, or footers to email, meeting invites, or documents that have the label applied. Watermarks can be applied to documents but not email or meeting invites. Example header and watermark:

Contoso Highly Confidential. Very sensitive data that will cause business harm if over-shared.

M&A Plan – "Bluefish"

Planning for next financial year, CONTOSO M&A DEPT

M&A ID: **CO0151502**

Microsoft

An M&A proposal regarding the potential merger with a company codenamed "Bluefish". Prepared by the Contoso Mergers & Acquisition sourcing department at Contoso, Ltd.

http://www.contoso.com

jpnshiken.com

Lorem ipsum dolor sit amet, natum putant constituto mei an. Eros homero semper te sed, eu pro quot veniam minimum, duo error euripidis cu. Et vix fugit errem principes, mei ei alienum voluptaria, sumo insolens posidonium at ius.

HIGHLY CONFIDENTIAL

Abstract

Pri nihil expetenda forensibus eu. Soleat verear utroque sea at, id stet commodo duo. Graece mediocritatem duo eu, eu qui dico causae instructior. Sea an meliore dolorem, duis lobortis quo ut, omnesque indoctum definiebas nam cu.

Pro soluta aliquid lucilius at, mei graecis qualisque eu. Sumo eruditi deterruisset est te, te sed error simul aliquam. Eos ut laoreet omittam, cum ei nostro graecis, doming



Step 6: Finish the Wizard
Reference:
https://learn.microsoft.com/en-us/purview/create-sensitivity-labels
https://answers.microsoft.com/en-us/msteams/forum/all/how-to-automatically-apply-sensitivity- labels-to/2482d1b2-1fe6-4a80-af4a-2b93b9c670de

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu **299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

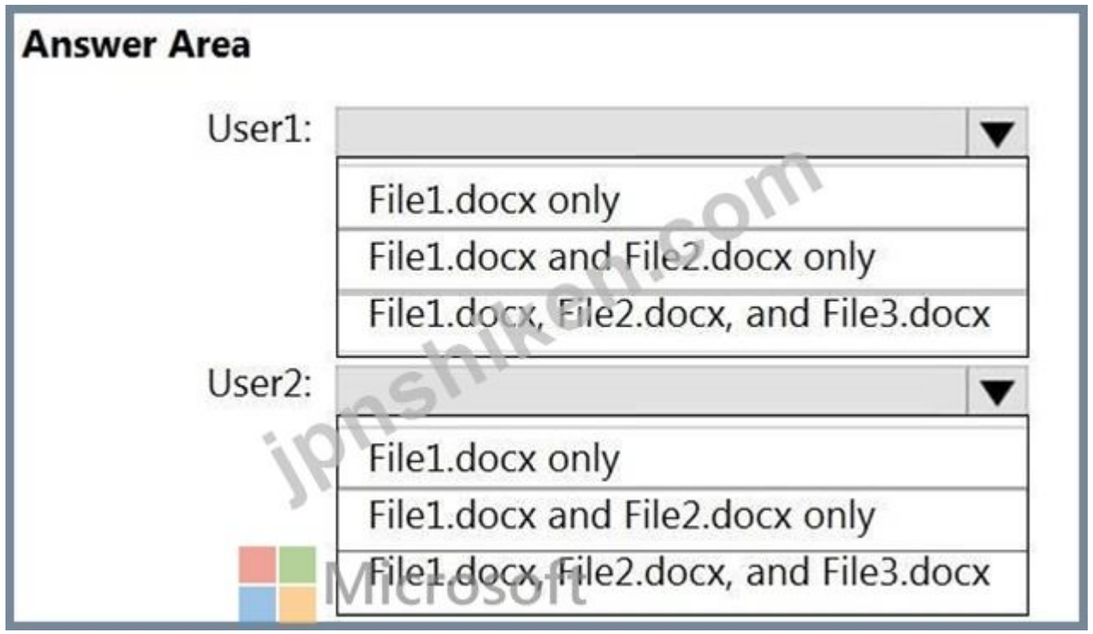
質問: **92**
ホットスポットに関する質問
次のファイルを含む Microsoft SharePoint Online サイトがあります。

Name	Modified by	Data loss prevention (DLP) status
File1.docx	Manager1	None
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

次の表に示すように、ユーザーにはサイトの役割が割り当てられます。

Name	Role
User1	Site owner
User2	Site member

User1 と User2 が開くことができるファイルはどれですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



Explanation:

User1: User1 is a Site Owner, meaning they have full control over all files in the site. Even though File3.docx is blocked by DLP, a Site Owner can override or manage DLP restrictions and still access all files.

User2: User2 is a Site Member, meaning they have standard permissions to view and edit files unless blocked. File1.docx has no DLP action, so User2 can access it. File2.docx is matched by DLP, but it is not blocked, so User2 can still access it. File3.docx is blocked by DLP, which means User2 cannot access it.

質問: 93

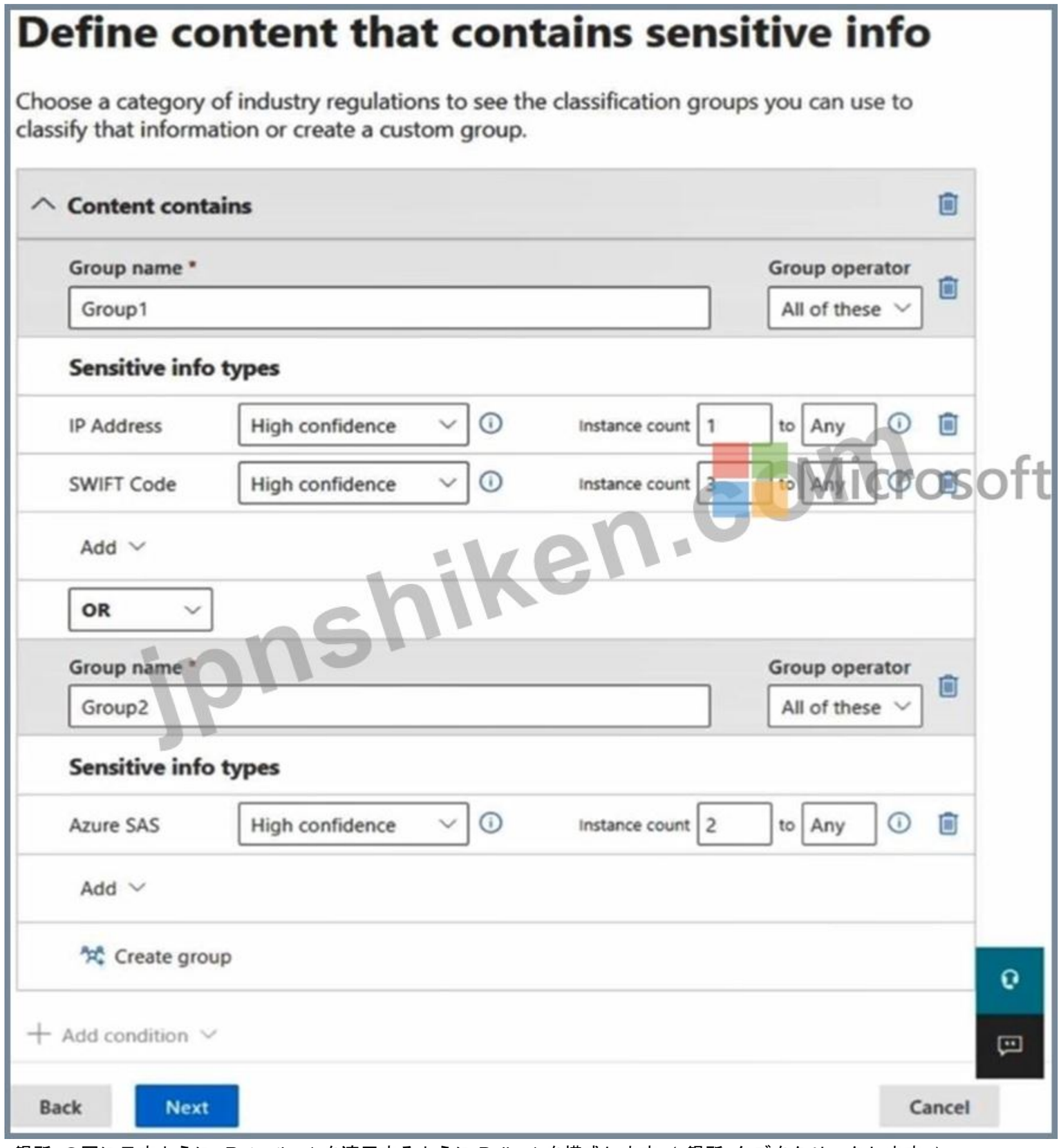
ホットスポットに関する質問

Retention1という保持ラベルを持つMicrosoft 365サブスクリプションがあります。このサブスクリプションには、次の表に示すファイルが含まれています。

Name	Stored in	Number of sensitive information types (SITs)		
		IP address	SWIFT code	Shared access signature (SAS)
File1	Microsoft Exchange Online	1	2	4
File2	Microsoft SharePoint Online	3	5	1
File3	Microsoft OneDrive	3	3	2

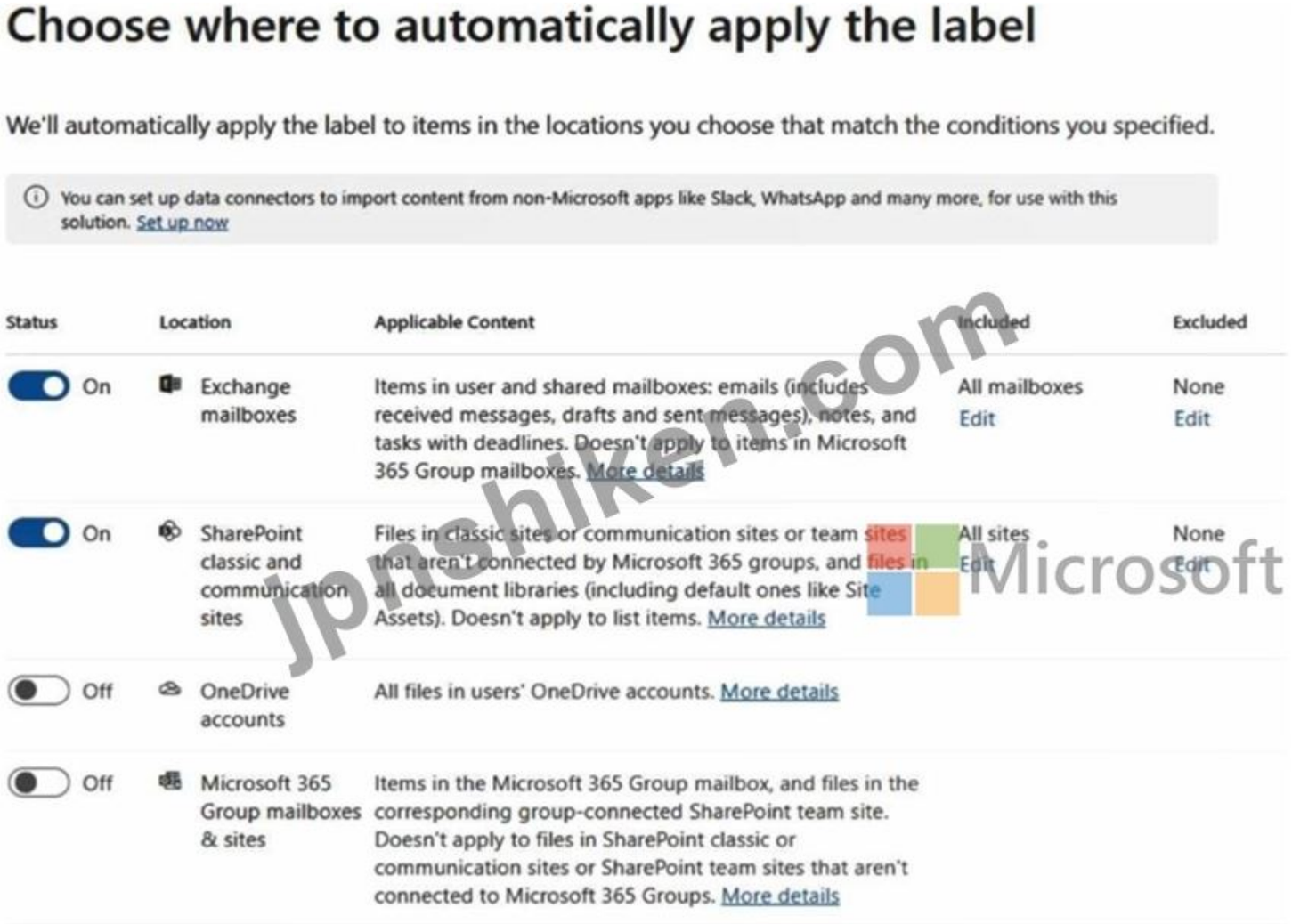
jpnshiken.com Microsoft

自動ラベル付けポリシーの図に示されているように、Retention1 を自動的に適用する Policy1 という名前の自動ラベル付けポリシーを作成します。([自動ラベル付けポリシー] タブをクリックします。)



jpnshiken.com Microsoft

場所」の図に示すように、Retention1 を適用するように Policy1 を構成します。(場所」タブをクリックします。)

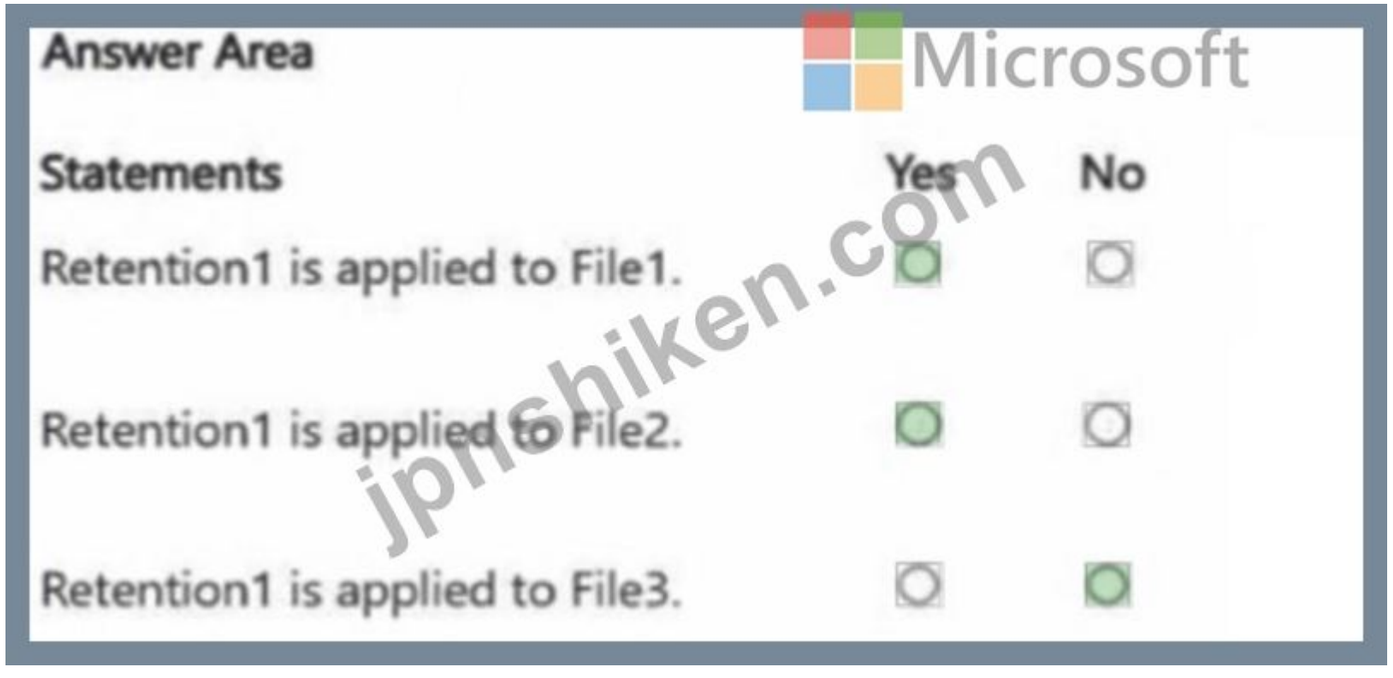


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:



jpnshiken.com

質問: **94**
Microsoft 365 E5 サブスクリプションをお持ちです。
データ損失防止 (DLP) ポリシーを作成し、選択します。
通知を使用してユーザーに通知し、機密情報の適切な使用について教育します。
どのアプリにポリシーヒントが表示されますか?
A. Web 上の Outlook のみ
B. Outlook Win32 のみ
C. iOS および Android 向け Outlook のみ
D. Web 上の Outlook および Outlook Win32 のみ
E. Outlook Win32 および iOS および Android 向け Outlook のみ
F. Web 上の Outlook、Outlook Win32、iOS および Android 向け Outlook
正解: **(**正解を表示します**)**
When you compose a new email in Outlook on the web and Outlook 2013 and later, you'll see a policy tip if you add content that matches a rule in a DLP policy, and that rule uses policy tips. The policy tip appears at the top of the message, above the recipients, while the message is being composed.
Note: Outlook Mobile (iOS, Android)/Outlook Mac: DLP policy tips are not supported on Outlook mobile Support Matrix for DLP policy tips across Microsoft apps.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-tips-reference
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips

質問: **95**
Microsoft 365 サブスクリプションをお持ちです。
今後 3 年間、次の監査ログ レコードの種類とアクティビティを保持する予定です。
- CopilotInteraction: すべてのアクティビティが選択されました (1/1)
- Copilotと対話した

- ComplianceDLPEndpoint: すべてのアクティビティが選択されました (2/2)
- 一致したDLPルール
- ドキュメントからDLPルールを削除しました
- AzureActiveDirectory: 25 個のアクティビティのうち 2 個が選択されました (2/25)
- ユーザーパスワードをリセットする
- ユーザーパスワードを変更しました
選択したレコードの種類とアクティビティのみを保持するために作成する必要がある監査保持ポリシーの最小数はいくつですか?
A. 1
B. 2
C. 3
D. 5
正解**: (**正解を表示します**)**
You only need one Microsoft 365 audit retention policy to cover CopilotInteraction, ComplianceDLPEndpoint, and AzureActiveDirectory for three years, as a single policy can be configured with a three-year duration to apply to all specified record types. However, this requires having a Microsoft 365 Enterprise E5 subscription and a 10-Year Audit Log Retention add-on license to meet the three-year retention requirement.
Reference:
https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

質問**: 96**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク9
次のキーワードを含むコンテンツに適用されるデータ損失防止 (DLP) ポリシーを作成する予定です。
- テールスピン
- 文学
- ファルコン
DLP ポリシーで使用できるキーワード リストを作成する必要があります。
正解**:**
To create a sensitive information type that matches all words in a keyword list, you can use the "All" condition instead of the default "Any" condition. Here are the steps to create such a sensitive information type:

Step 1: Go to the Microsoft 365 compliance center and navigate to the "Sensitive information types" page.
Step 2: Click on "Create a sensitive information type".
Step 3: Choose "Keyword dictionary" as the type of sensitive information you want to create.
Step 4: Enter a name and description for the sensitive information type.
Step 5: In the "Keywords" section, enter all the words you want to match separated by com-mas.
Here we enter: Tailspin, Litware, Falcon
Step 6: Click on "Add condition" and choose "Any" as the condition type.
Step 7: Click on "Create" to create the sensitive information type.
Step 8: Click on "Create" to create the sensitive information type.
With this configuration, the DLP policy will only detect the sensitive information if any the words in the keyword list are present in the content being scanned.
Reference:
https://learn.microsoft.com/en-us/answers/questions/1419105/how-to-create-sensitive- information-types-to-match

質問**: 97**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーがデータ損失防止 (DLP) で保護されたドキュメントを次のサードパーティの Web サイトにアップロードできないようにする必要があります。
web1.contoso.com
web2.contoso.com
ソリューションでは管理上の労力を最小限に抑える必要があります。
エンドポイント DLP のサービス ドメイン設定を何に設定する必要がありますか?
A. *.contoso.com
B. contoso.com
C. web1.contoso.com と web2.contoso.com
D. web*.contoso.com
正解**: (**正解を表示します**)**
The Service domains setting in Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) allows administrators to block or allow specific domains for file uploads. The goal is to prevent users from uploading DLP-protected documents to web1.contoso.com and web2.contoso.com.
Setting the Service domains to "web1.contoso.com and web2.contoso.com" precisely targets the two specific third-party websites, minimizing administrative effort while ensuring strict control.

質問**: 98**
User1 という名前のユーザーを含む Microsoft 365 サブスクリプションがあります。
User1 は、Microsoft Purview 通信コンプライアンス ポリシーの変更履歴をエクスポートする予定です。
Microsoft Purview のロールグループに User1 を追加する必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 をどの役割グループに追加する必要がありますか?
A. コミュニケーションコンプライアンス調査員
B. コミュニケーションコンプライアンス閲覧者
C. コミュニケーションコンプライアンスアナリスト
D. コミュニケーションコンプライアンス管理者
正解**: (**正解を表示します**)**
https://learn.microsoft.com/en-us/purview/communication-compliance-configure?tabs=purview- portal

質問: **99**
Site1 と Site2 という名前の 2 つの Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
Label1 という名前の保持ラベルを構成し、Site1 内のすべてのファイルに Label1 を適用する予定です。
Site1 にファイルが作成されてから 2 年後に、そのファイルが自動的に Site2 に移動されるようにする必要があります。
Label1 の 「保持期間後の処理を選択する」設定をどのように構成すればよいですか?
A. 保持設定を無効にする
B. Power Automateフローを実行する
C. 処分レビューを開始する
D. ラベルを変更する
正解: (正解を表示します)
Common settings for retention policies and retention label policies
Selecting Run a Power Automate flow enables moving labeled items to be moved to a certain location.
Reference:
https://learn.microsoft.com/en-us/purview/retention-settings

質問: **100**
Microsoft 365 E5 サブスクリプションがあり、User1 と User2 という 2 人のユーザーが登録されています。このサブスクリプションには、Policy1 というデータ損失防止 (DLP) ポリシーが設定されています。
User2 は、Policy1 に対して誤検知を生成する送信メッセージを送信します。
User1 がアラートを生成したメッセージをダウンロードできるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 をどの役割グループに追加する必要がありますか?
A. データ調査員
B. セキュリティオペレーター
C. 電子情報開示マネージャー
D. グローバルリーダー
正解: (正解を表示します)
Global Reader
Members have read-only access to reports, alerts, and can see all the configuration and settings.
Roles include:
* View-Only DLP Compliance Management
Reference:
https://learn.microsoft.com/en-us/defender-office-365/scc-permissions

質問: **101**
Microsoft 365 E5 テナントがあります。
新しいキーワード辞書を追加する必要があります。
何を創造すべきでしょうか?
A. 機密ラベル
B. 保持ポリシー
C. 機密情報の種類
D. 学習可能な分類器

正解: (正解を表示します)

質問: **102**

Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーと、File1.docx という名前のファイルが含まれています。

次の図に示すように、Label1 という名前の機密ラベルを作成します。



Label1 を File1 に適用します。

Microsoft 365 Copilot はどのユーザーに対して File1 を要約できますか?

A. ユーザーなし

B. ユーザー1のみ

C. ユーザー1とユーザー2のみ

D. ユーザー1、ユーザー2、ユーザー3

正解: (正解を表示します)

When the sensitivity label applies encryption, the user must have the EXTRACT and VIEW usage rights for Copilot to summarize the data.

User1 - Yes

User1 is Co-Author.

Microsoft 365 co-authors typically have both view and extract permissions when working on documents collaboratively. Co-authors can view and edit the document, and also copy and extract content from it, depending on the specific permissions granted.

User2 - No

A "Reviewer" role generally has view permissions, but not necessarily extract permissions.

Reviewers can typically view the content of documents, files, or other resources, and often can add comments or make tracked changes (depending on the specific implementation and settings). However, they may not have the ability to download or export the content, unless explicitly granted those rights.

User3 - No

User3 has only view permission, not extract permissions.

Note:

Jpnshiken.com

If a user is the owner of a sensitivity label and that label is applied to a file, Microsoft 365 Copilot can summarize the file for that user, provided the user also has the necessary usage rights, specifically EXTRACT and VIEW, granted by the sensitivity label, according to Microsoft Learn. If the label includes encryption, these usage rights become crucial for Copilot's ability to access and summarize the content.
Reference:
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data- protection-auditing

質問: **103**
ケーススタディ 1 - Contoso 社
概要
Contoso 社は、モントリオールに本社を置き、シアトル、ボストン、ヨハネスブルグに 3 つの支社を持つコンサルティング会社です。
既存の環境
Microsoft 365 環境
Contoso 社には Microsoft 365 E5 テナントがあります。このテナントには、次の表に示す管理ユーザーアカウントが含まれています。

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

ユーザーは次の場所にデータを保存します。
- SharePoint サイト
- OneDriveアカウント
- Exchangeメール
- Exchangeパブリックフォルダ
- Teamsチャット
- Teams チャネル メッセージ
研究部門のユーザーが文書を作成する際は、各文書に10桁のプロジェクトコードを追加する必要があります。999で始まるプロジェクトコードは機密情報です。
SharePoint Online 環境
Contoso には、Site1、Site2、Site3、Site4 という名前の 4 つの Microsoft SharePoint Online サイトがあります。
Site2 には、次の表に示すファイルが含まれています。

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

次の表に示すように、User1 と User2 という名前の 2 人のユーザーに Site2 のロールが割り当てられています。

User	Role
User1	Site owner
User2	Site visitor

Site3には、会社のプロジェクトに関連する文書が保存されています。文書はプロジェクトごとにフォルダ階層に整理されています。
Site4 には次の 2 つの保持ポリシーが適用されています。
- 名前: Site4RetentionPolicy1
ポリシーを適用する場所: サイト4
2年以上前のアイテムを削除
コンテンツを削除する基準: アイテムが作成された日時
- 名前: Site4RetentionPolicy2
ポリシーを適用する場所: サイト4
特定の期間アイテムを保管する: 4 年間
保存期間の開始基準: アイテムが作成された日時
保存期間の終了時: 何もしない
問題ステートメント
Contoso社の経営陣はデータ漏洩を懸念しています。研究部門の機密文書が漏洩するケースが複数回発生しました。
要件
計画された変更
Contoso では、次のデータ損失防止 (DLP) ポリシーを作成する予定です。
- 名前: DLPpolicy1
ポリシーを適用する場所: サイト2
条件：
コンテンツには、次のいずれかの機密情報タイプが含まれています: SWIFT コード
- インスタンス数: 2～任意
アクション: コンテンツへのアクセスを制限する
技術要件
Contoso は次の技術要件を満たす必要があります。
- すべての管理ユーザーは DLP レポートを確認できる必要があります。
- 可能な限り、最小権限の原則を使用する必要があります。
- すべてのユーザーについて、Microsoft 365のデータは少なくとも
1年。
- 機密文書は、以下の方法で検出し保護する必要があります。
マイクロソフト365。
- クレジットカード番号を含むサイト1文書にはラベルを付ける必要がある
自動的に。
- すべての管理ユーザーはMicrosoft 365を作成できる必要があります
機密ラベル。
- プロジェクトが完了したら、サイト3にある関連する文書は
プロジェクトは10年間保持する必要があります。
ホットスポットに関する質問

DLPpolicy1 をオンにした後、User1 と User2 は Site2 内のいくつのファイルにアクセスできますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Microsoft
jpnshiken.com

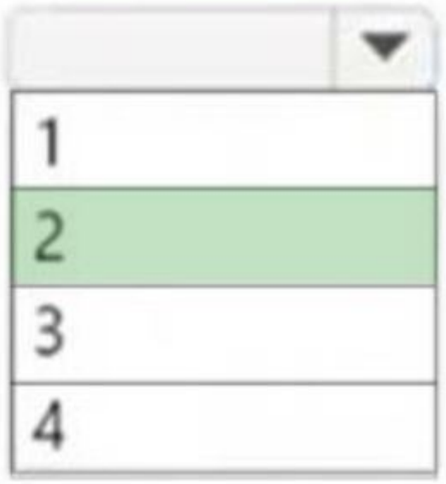
正解:

Answer Area

Number of files that User1 can access:



Number of files that User2 can access:



Microsoft
jpnshiken.com

Explanation:
User 1 (Site Owner) - 4 Files
User 2 (Site Visitor) 2 Files
Any item that makes it through the conditions filter has any actions that are defined in the rule applied to it. You have to configure the required options to support the action. For example, if you select Exchange with the Restrict access or encrypt the content in Microsoft 365 locations action, you need to choose from these options:
Block users from accessing shared SharePoint, OneDrive, and Teams content Block everyone. Only the content owner, last modifier, and site admin will continue to have access Block only people from outside your organization. Users inside your organization continue to have access.
Encrypt email messages (applies only to content in Exchange)
The actions that are available in a rule depend on the locations that have been selected. The available actions for each individual location are listed below.
https://learn.microsoft.com/en-us/purview/dlp-policy-reference#actions

質問: **104**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com" を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク4
一般データ保護規則 (GDPR) のデータ損失防止 (DLP) ポリシーによって生成される誤検知の数を減らす必要があります。
正解:
To reduce false-positives with a GDPR DLP policy, run the policy in audit-only mode first to identify issues, continuously refine the rules based on this data, and train employees on proper data handling.
To run an existing GDPR DLP policy in audit mode, you need to edit the policy in your Microsoft Purview portal and set the policy mode to "simulation" or "test". In the policy configuration, select the option to "Run the policy in simulation mode" or "Test mode" instead of enabling enforcement immediately. This will log any violations without blocking them, allowing you to review the results before a full deployment.
Steps to run a policy in audit (simulation) mode
Step 1: Navigate to DLP policies: Sign in to the Microsoft Purview portal and go to Data loss prevention > Policies.
Step 2: Edit the policy: Select the existing GDPR policy you want to run and choose to edit it.
Step 3: Locate the policy mode settings: In the policy configuration workflow, find the page for policy mode, which may be labeled as "Policy Mode" or "Simulate or turn on the policy".
Step 4: Enable simulation mode: Choose the option to "Run the policy in simulation mode".
Step 5: Configure optional settings: You can also choose to "Show policy tips" in simulation mode to help educate users about potential violations without actually blocking them. [Skip] Step 6: Save and submit: Proceed through the rest of the wizard and select Next and Submit to save your changes.
Reference:
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp

質問: **105**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview ポータルを使用して、インサイダー リスク管理ポリシーで使用する人事 (HR) データをマッピングする予定です。
HR データをインポートするには、データ コネクタを追加する必要があります。
最初に何をすべきでしょうか、またどのような形式でデータをインポートすべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

Answer Area

First:
- Configure the Insider risk management settings.
- Create a new import job in the Data lifecycle management settings.
- Create a subject rights request.
- Register an app in Microsoft Entra ID.

Import as:
- CSV
- XLSX
- XML
- ODS

正解:

Answer Area

First:
- Configure the Insider risk management settings.
- Create a new import job in the Data lifecycle management settings.
- Create a subject rights request.
- Register an app in Microsoft Entra ID.

Import as:
- CSV
- XLSX
- XML
- ODS

Explanation:

Step 1: Prepare a CSV file with your HR data

Step 2: Create an app in Microsoft Entra ID

Step 3: Create the HR connector
Step 4: Run the sample script to upload your HR data
Step 5: Monitor the HR connector
(Optional) Step 6: Schedule the script to run automatically
(Optional) Step 7: Upload data by using Power Automate templates
Reference:
https://learn.microsoft.com/en-us/purview/import-hr-data

質問: **106**
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
SIT1 という名前の機密情報の種類 (SIT) を作成します。
次の表に示す通信コンプライアンス ポリシーを作成する予定です。

Name	Template used
Policy1	Detect inappropriate text
Policy2	Detect inappropriate image
Policy3	Detect conflict of interest

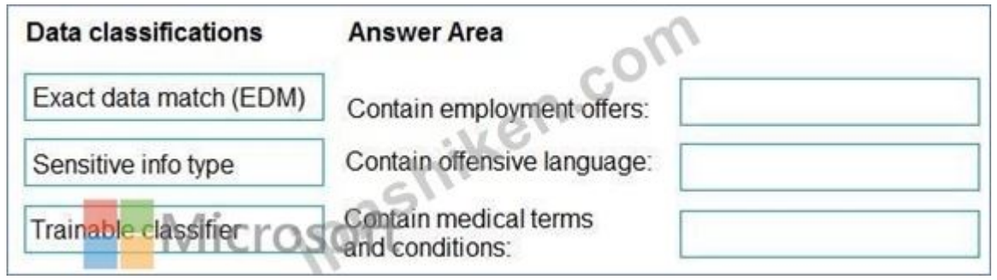
SIT1 を条件として追加できるポリシーはどれですか?
A. ポリシー3のみ
B. ポリシー1、ポリシー2、およびポリシー3
C. ポリシー1とポリシー2のみ
D. ポリシー1とポリシー3のみ
E. ポリシー1のみ
正解: (正解を表示します)

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

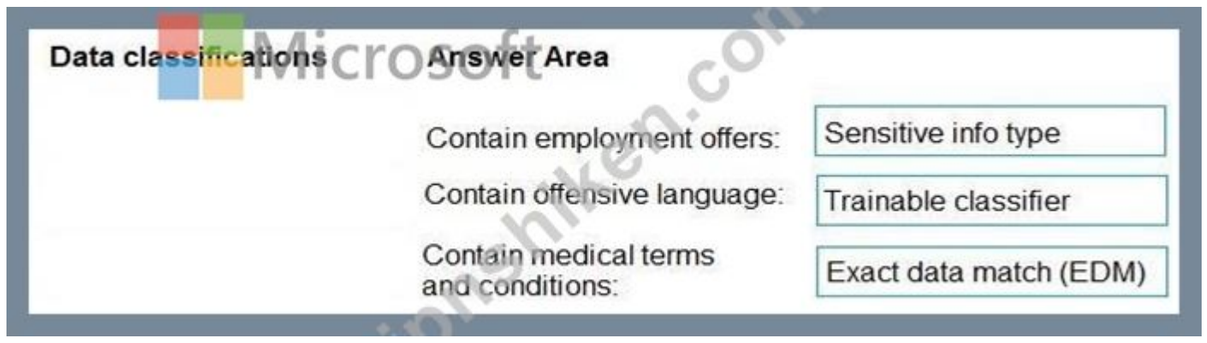
質問: **107**
500 台の Windows デバイスを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Purview Data Security Posture Management for AI (DSPM for AI) を展開する予定です。
サードパーティの生成 AI ウェブサイトでのユーザー アクティビティを監視できることを確認する必要があります。
DSPM for AI に必要な前提条件のうち、どれを 2 つ満たすべきですか? 正解はそれぞれソリューションの一部を示します。注: 正解の選択はそれぞれ 1 ポイントの価値があります。
A. エンドポイント データ損失防止 (エンドポイント DLP) ポリシーを作成します。
B. デバイスを Microsoft Purview にオンボードします。
C. デバイスに Microsoft Purview 拡張機能をインストールします。
D. 通信コンプライアンス ポリシーを作成します。
E. デバイスを Microsoft Intune に登録します。

F. データ漏洩ポリシーを作成します。
正解**:** (正解を表示します)
Required for monitoring interactions with third-party generative AI sites:
[B] * Devices are onboarded to Microsoft Purview, required for:
- Gaining visibility into sensitive information that's shared with third-party generative AI sites. For example, a user pastes credit card numbers into ChatGPT.
[A]- Applying endpoint DLP policies to warn or block users from sharing sensitive information with third-party generative AI sites. For example, a user identified as elevated risk in Adaptive Protection is blocked with the option to override when they paste credit card numbers into ChatGPT.
Reference:
https://learn.microsoft.com/en-us/purview/dspm-for-ai-considerations

質問**: 108**
ドラッグアンドドロップの質問
Microsoft 365 E5 サブスクリプションをお持ちです。
次の条件に一致する Microsoft Exchange Online 電子メールにラベルを付ける必要があります。
- 雇用オファーを含む
- 不快な言葉が含まれている
- 医療用語が含まれている
ソリューションでは管理上の労力を最小限に抑える必要があります。
各条件にはどのタイプのデータ分類を使用すべきでしょうか？適切なデータ分類タイプを正しい条件にドラッグしてください。各データ分類タイプは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解**:**



Explanation:
Reference:
https://learn.microsoft.com/en-us/purview/classifier-learn-about
https://learn.microsoft.com/en-us/purview/classifier-tc-definitions

https://learn.microsoft.com/en-us/purview/sit-learn-about-exact-data-match-based-sits

質問: **109**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク7
次の要件を満たす保持ポリシーを作成する必要があります。
- Microsoft Teams チャットと Teams チャネル メッセージに適用されます。
- アイテムは作成日から 5 年間保持され、その後削除されます。
正解:
Stage 1: Create an adaptive scope
Step 1: Sign into Microsoft Purview compliance portal using credentials for an admin account in your Microsoft 365 organization.
Step 2: In the compliance portal, select Roles and Scopes.
Step 3: Select Adaptive scopes, and then + Create scope.
Step 4: Follow the prompts in the configuration where you'll first be asked to assign an administrative unit. If your account has been assigned administrative units, you must select one administrative unit that will restrict the scope membership. (Does not apply here) If you don't want to restrict the adaptive scope by using administrative units, or your organization hasn't configured administrative units, keep the default of Full directory. (Applies here) Step 5: Select the type of scope, and then select the attributes or properties you want to use to build the dynamic membership, and type in the attribute or property values. Select Add attribute (for users and groups).
For example, to configure an adaptive scope that will be used to identify users in Europe, first select Users as the scope type, and then select the Country or region attribute, and type in Europe:
Step 6: For User Attributes select: Department, is equal to, Sales
Stage 2: Create and configure retention policies
Step 1: From the Microsoft Purview compliance portal, select Data lifecycle management > Microsoft 365 > Retention Policies.
Step 2: Select New retention policy to start the Create retention policy configuration, and name your new retention policy.
Step 3: For the Assign admin units page (skip)
Step 4: For the Choose the type of retention policy to create page, select Adaptive or Static.
Select Adaptive.
We need Adaptive scopes.
Step 5: On the Choose adaptive policy scopes and locations page, select Add scopes and select the one you created in Stage 1.



Step 6: Then, select one or more locations. The locations that you can select depend on the scope types added. For example, if you only added a scope type of User, you'll be able to select Teams chats but not Teams channel messages.

Select: Teams chat and Teams channel

Step 7: For Decide if you want to retain content, delete it:

Select: On the Decide if you want to retain content, delete it, or both page, select Retain items for a specific period, specify the retention period [specify 5 years], and then for At end of the retention period select Delete items automatically.

Note: We need to retains item for five years from the date they are created, and then deletes them.

Reference:

https://learn.microsoft.com/en-us/purview/purview-adaptive-scopes

https://learn.microsoft.com/en-us/purview/create-retention-policies

https://learn.microsoft.com/en-us/purview/retention-settings#settings-for-retaining-and-deleting- content

質問**: 110**

次の表に示すファイルを含む、Site1 という名前の Microsoft SharePoint Online サイトがあります。

Name	Number of IP addresses in the file
File1	2
File2	3

次の表に示す高度な DLP ルールを持つ、DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

DLP1 を Site1 に適用します。

File2 にはどのようなポリシーヒントが表示されますか?

A. ヒント1のみ

B. ヒント2のみ
C. ヒント3のみ
D. ヒント1とヒント2のみ
正解: **(**正解を表示します**)**
It's possible for content to match several rules in a DLP policy, but only the policy tip from the most restrictive, highest-priority rule will be shown. For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy- tips?view=o365-worldwide

質問: **111**
Microsoft 365 サブスクリプションをお持ちです。
Policy1 という名前の Microsoft Purview インサイダー リスク管理ポリシーを構成します。
ポリシー1の指標しきい値の設定方法に関する推奨事項をリアルタイムで確実に受け取る必要があります。このソリューションでは、推奨事項が過去10日間のユーザーアクティビティに基づいていることが保証される必要があります。
まず何をすべきでしょうか?
A. Insider リスク インジケーター コネクタを作成します。
B. Insider リスク管理データ共有設定を構成します。
C. データ損失防止 (DLP) ポリシーを作成する
D. インサイダー リスク管理分析を有効にします。
正解: **D (**コメントを発表する**)**
Prerequisites for using real-time analytics
To use real-time analytics (preview), you must enable insider risk analytics insights. After analytics is enabled, it can take 24 to 48 hours for insights and recommendations to appear.
Note: Adjust threshold settings manually
If you select the Choose your own thresholds option and manually adjust a threshold setting for a specific indicator, the insight below the indicator updates in real time. This helps you configure the appropriate thresholds for each indicator to achieve the highest level of alert effectiveness before activating your policies.
Reference:
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators

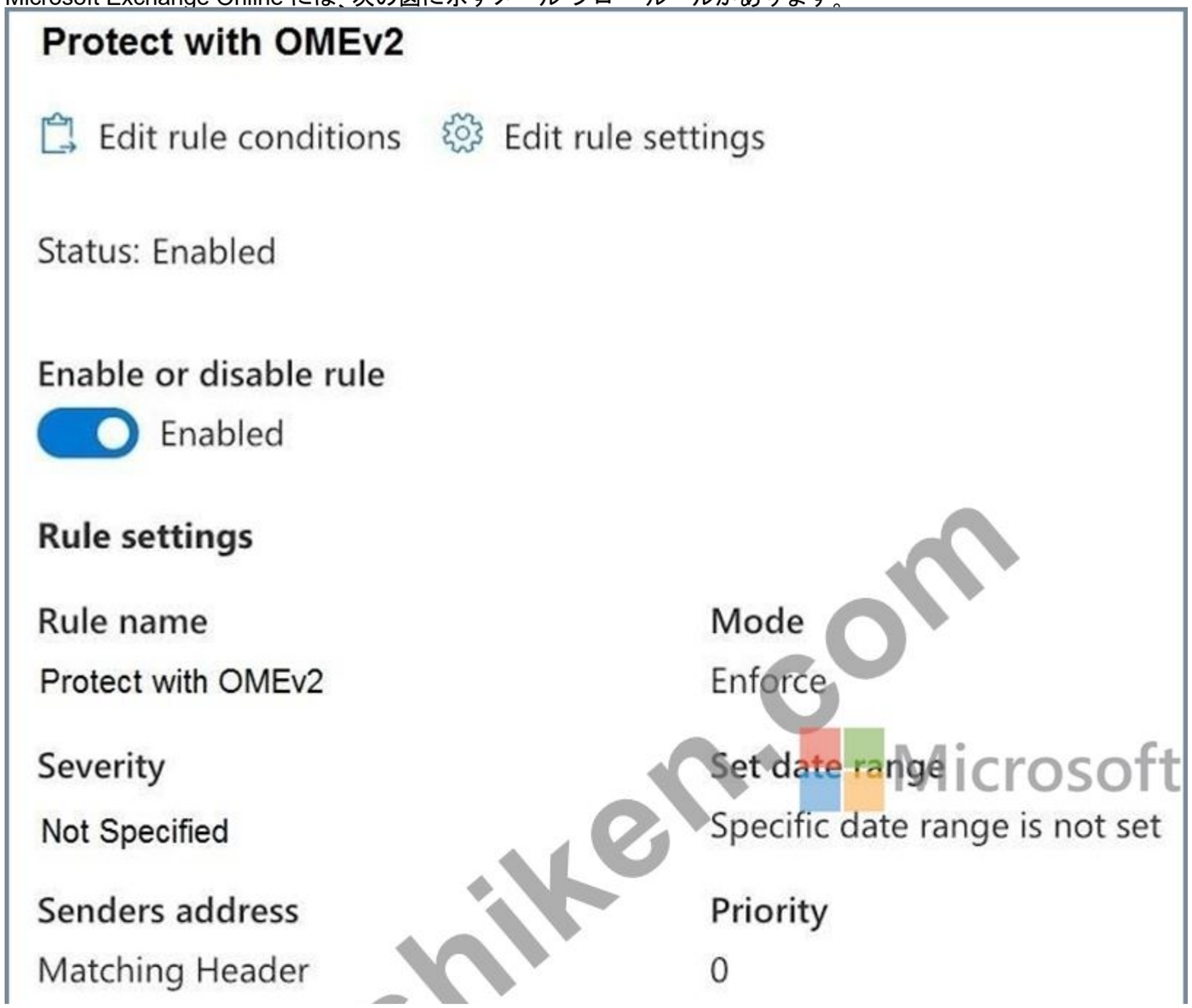
質問: **112**
Trainable1 という名前のトレーニング可能な分類子を含む Microsoft 365 E5 サブスクリプションがあります。
次の表に示す項目を作成する予定です。

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Trainable 1 を使用できるアイテムはどれですか?
A. ラベル2のみ
B. ラベル1とラベル2のみ
C. ラベル1とポリシー1のみ
D. ラベル2、ポリシー1、DLP1のみ
E. ラベル1、ラベル2、ポリシー1、およびDLP1

正解: (正解を表示します)
A trainable classifier in Microsoft Purview is used to automatically identify and classify unstructured data based on content patterns. The classifier can be used in:
1. Retention Labels (Label2) Supported
Trainable classifiers can be linked to retention labels to automatically classify and apply retention policies to documents.
2. Retention Label Policies (Policy1) Supported
Retention label policies define how and where retention labels are applied, including automatically using trainable classifiers.
3. Data Loss Prevention (DLP) Policies (DLP1) Supported
Trainable classifiers can be used in DLP policies to detect and protect sensitive content automatically.

質問: **113**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Exchange Online には、次の図に示すメール フロー ルールがあります。



chiken.com
Microsoft

For rule processing errors

Ignore

Rule description

Apply this rule if

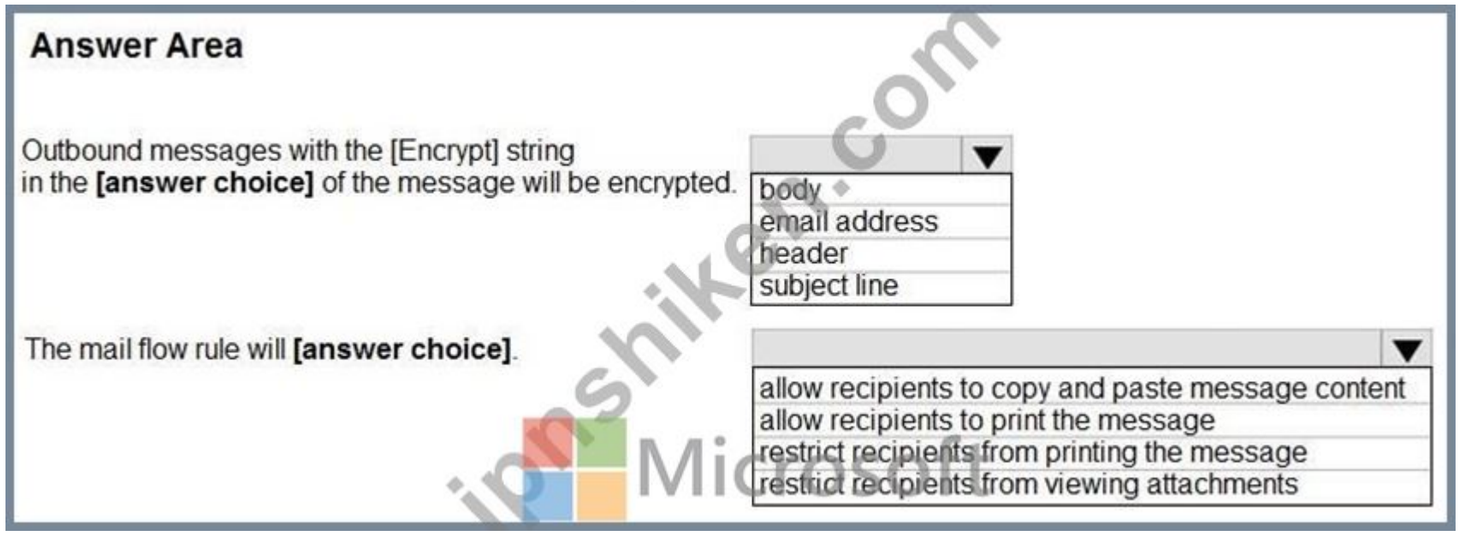
Is sent to 'Outside the organization'
and includes these words in the message subject '[Encrypt]'

Do the following

rights protect messages with RMS template: 'Do Not Forward'

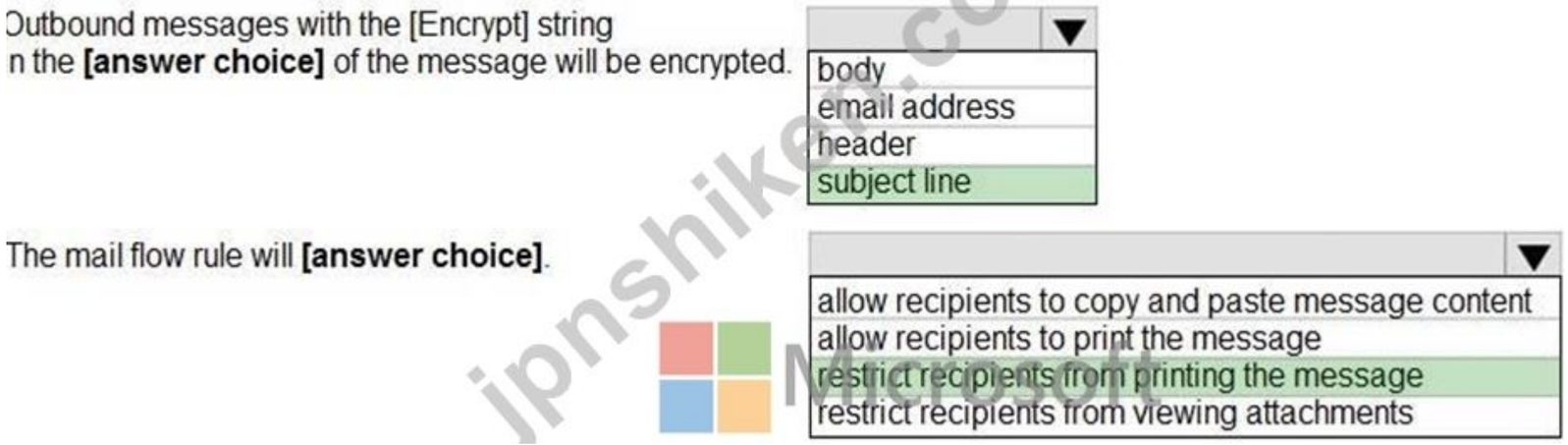
Rule comments

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



正解:

Answer Area



ipnshiken.com
Microsoft

Explanation:

Box 1: subject line

Box 2: restrict recipients from printing the message

Note: IRM is an encryption solution that also applies usage restrictions to email messages. It helps prevent sensitive information from being printed, forwarded, or copied by unauthorized people.

IRM capabilities in Microsoft 365 use Azure Rights Management (Azure RMS).

Reference:

https://learn.microsoft.com/en-us/purview/email-encryption

有効的な**SC-401J**問題集はJPNTest.com提供され、**SC-401J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-401J**試験問題集を提供します。JPNTest.com SC-401J試験問題集はもう更新されました。ここで**SC-401J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-401J-mondaishu　**299**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」