Purview DLP Setup Runbook

Purview DLP セットアップランブック

April 11, 2026 / 2026 年 4 月 11 日

English Version

See page 26 →

日本語版

4 ページへ →

Purview DLP セットアップランブック

2026 年 4 月 11 日

目次

> eSolia INTERNAL — Not for distribution outside eSolia

eSolia 自社テナントに Microsoft Purview Data Loss Prevention を展開するためのステップバイステップ手順書です。前提条件の検証、eSolia ベースライン全 5 ルール、コンサルティングオーバーレイ 4 項目、選択した SMB 項目（退職予定者監視、軽量デバイス制御）をカバーします。フェーズ展開込みで 4〜6 週間にまたがる、合計 6〜10 時間の作業を見込んでください。

開始する前に

このランブックは `eSolia-Purview-DLP-Baseline-Policy-Reference-INTERNAL-20260411-ja.md`（「何を、なぜ」のリファレンス）の「どうやって」版です。各ポリシーの背景については先にリファレンスを読んでください。本文書は、eSolia テナント特有のクリックパス、正確な設定値、操作順序にフォーカスしています。

必要なもの：

- **Compliance Administrator と Security Administrator ロールが付与された管理者アカウント**、PIM を使っている場合は activate 済みであること
- **Microsoft Purview ポータル**（`https://purview.microsoft.com`）の作業セッション、eSolia テナントコンテキストが確認済みであること（URL に `tid=436f19ac-627e-4ec1-bfcb-7404d06a5b46`）
- **PowerShell が使えるマシン**、Microsoft Graph と ExchangeOnlineManagement モジュールがインストール済み（前提条件検証ステップで使用）
- **初回展開セッションに約 90 分**、その後数週間にわたるフェーズ移行とチューニングのチェックイン時間
- **テスト用ユーザーアカウント** 1 つ。普段使いのアカウントとは別に。自分の監査証跡を汚さずに検証するため

妥当なロールアウトスケジュール：1 日目に前提条件検証とフェーズ 1（audit mode）を実施（90 分）。2 週間 Activity Explorer を観察。14 日目にフェーズ 2（notify mode）を実施（30 分）。さらに 2 週間観察して質問対応。28 日目にフェーズ 3（enforce）を実施（30 分プラスユーザーへの周知）。それ以降は定常運用。

フェーズ 0：前提条件の検証

これは飛ばさないでください。Purview 展開で失敗する原因のほとんどは、誰かが前提条件が満たされていると思い込んだのに実際は満たされていなかったというものです。検証は 15〜20 分で済み、デバッグの数時間を節約します。

Step 0.1: ライセンスを確認

```
Connect-MgGraph -Scopes "Organization.Read.All","Directory.Read.All"
Get-MgSubscribedSku | Select SkuPartNumber, ConsumedUnits,
@{N='Enabled';E={$_.PrepaidUnits.Enabled}}
```

少なくとも以下のいずれかが見えるはずです：

- `SPE_E5`（Microsoft 365 E5）
- `INFORMATION_PROTECTION_COMPLIANCE`（M365 E5 Compliance アドオン）
- `M365_E5_INFO_PROTECTION_GOVERNANCE`（M365 E5 IP&G アドオン）

どれもない、または数がゼロなら、ここで停止します。ベースラインは E5 レベルの Information Protection 機能を前提にしています。それなしでも一部（基本 SIT、手動 sensitivity label、基本 DLP）は展開できますが、endpoint DLP、trainable classifier、auto-labeling、Insider Risk Management が使えません。ベースラインの価値の大部分が失われます。

eSolia 固有の事情：2026 年現在、リックと一部の管理者・IT 担当ユーザーが E5 を持っており、その他のスタッフは E3 です。ベースラインポリシーはテナントに適用するためこれで問題ありません。エンドユーザーは、自分が触れる機能のライセンスが必要です：sensitivity label（手動適用は E3 で十分、auto-labeling は E5）、endpoint DLP（E5）など。E3 ユーザーで silent fail するポリシーを展開しないよう、ユーザー単位のライセンス制約を文書化しておいてください。

Step 0.2: Endpoint DLP デバイスモニタリングがオンか確認

Purview ポータルで：

1. Settings（右上の歯車アイコン）→ Device onboarding → Devices
2. **「Turn off Windows device monitoring」** と **「Turn off macOS device monitoring」** が表示されていることを確認（オフにするボタンが見えるということは、現在オンになっている。「Turn on…」が見えるならオフ）
3. macOS モニタリングがオフなら、**「Turn on macOS device monitoring」** をクリックし、有効化まで最大 30 分待つ
4. 自分の Mac（`ESO-LYXN42490K` または現在のデバイス名）がデバイスリストに表示され、Configuration status = Updated、Endpoint DLP status = Enabled になっていることを確認

自分の Mac がリストに無いか、健全でない場合は、ここで停止して `eSolia-Defender-macOS-DLP-Troubleshooting-Runbook-INTERNAL-20260410-ja.md` で修正してください。技術的には、全デバイスのオンボード前に DLP ポリシーを展開できます。報告中のサブセットだけに適用されます。ただし、何かを enforce に切り替える前に、少なくとも 1 台の健全なデバイスで検証したい。

Step 0.3: Advanced Audit が有効か確認

```
Connect-ExchangeOnline
Get-AdminAuditLogConfig | Select UnifiedAuditLogIngestionEnabled
```

`True` を返すべきです。`False` の場合は有効化：

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

これは 1 行で済みますが、イベントの取り込みが始まるまで最大 24 時間かかります。すでにオンなら何もしなくて良い。

Step 0.4: Pay-as-you-go billing リンクの確認（任意だが推奨）

Purview ポータルで：Settings → DLP → Billing。黄色のバナーで Azure サブスクリプションのリンクが必要と表示されたら、リンクの指示に従ってください。eSolia のベースラインでは下記のルールに pay-as-you-go は厳密には不要ですが、新しめの Purview 機能（advanced classification、EDM、一部の自動化）はリンクなしでは silent no-op になります。必要になる前に設定しておく価値があります。

Step 0.5: eSolia ラベル分類体系の確認または作成

ベースラインは 7 層の sensitivity label 分類体系を前提にしています。現状を確認：

```
Connect-IPPSSession
Get-Label | Select DisplayName, Identity, ParentLabelDisplayName | Sort DisplayName
```

eSolia では、以下の 7 つの親ラベルが存在する（または作成しようとしている）はずです：

優先度	内部名	表示名（EN）	表示名（JA）
0	`eSolia-Public`	Public	社外一般
1	`eSolia-WorkShare`	Work Share	業務共有
2	`eSolia-CommercialPapers`	Commercial Papers	商用書類
3	`eSolia-ProtectedInternal`	Protected Internal	社内一般
4	`eSolia-ClientConfidential`	Client Confidential	顧客機密情報
5	`eSolia-Confidential`	Confidential	秘密
6	`eSolia-Restricted`	Restricted	極秘

これらが存在しない場合は、Purview ポータル → Solutions → Information Protection → Labels → Create a label で作成してください。各ラベルで以下を設定：

- **EN と JA の両方の表示名**（日本語版の Office を使うユーザーには日本語名が表示される）
- 適用タイミングを説明する **両言語のツールチップ**

- Confidential と Restricted の **暗号化設定**（Microsoft-managed key、デフォルトで「組織内の全ユーザー」向けに暗号化）
- Restricted の **コンテンツマーキング**：ヘッダーテキスト「Restricted / 極秘 — eSolia INTERNAL」
- **Endpoint data protection**（ラベルと DLP ルールを接続する重要部分）
- **ファイルとメールへの auto-labeling** — 初期はオフ。ラベル公開後に有効化する

その後、Purview ポータル → Solutions → Information Protection → **Label policies** → Create policy で公開。7 つのラベルすべてを全ユーザーに公開し、`eSolia-ProtectedInternal` を新規ドキュメントのデフォルトに設定し、ラベルダウングレード時に justification を要求します。

> **重要：** 上記の 7 層分類体系は eSolia Standards MCP に文書化済みです。本ドキュメントはその正式版を参照しています。Standards MCP で分類体系が更新された場合は、このランブックも合わせて更新してください。

Step 0.6: サポート用 Entra ID グループの作成

このランブックはいくつかのセキュリティグループを参照します。フェーズ 1 開始前に Entra ID で作成してください。すべて **assigned**（dynamic ではない）、**security** タイプ：

- `eSolia-DLP-Bypass-Documentation` — サンプル認証情報を含むドキュメントを作成する必要があるユーザー。マーケティング・コンテンツチームと自分を追加。
- `eSolia-DLP-Finance-Exception` — 金融データを正当に社内で扱うユーザー。経理・財務スタッフを追加。
- `eSolia-DLP-Legal-Exception` — 契約テンプレートと法務文書を正当に扱うユーザー。法務レビュー責任者を追加。
- `eSolia-Departing-Employees` — 当面は空。退職通知が出された時点で HR が登録する。HR の offboarding チェックリストに記載。
- `eSolia-MNPI-Authorized` — 当面は空。eSolia は現状おそらく MNPI を直接扱わないが、将来のために存在させておく。

各グループの目的を description フィールドに記録し、将来の管理者がなぜ存在するか分かるようにしてください。

フェーズ 0 サインオフチェックリスト

フェーズ 1 に進む前に、以下すべてを確認：

- □ 少なくとも管理者ユーザーに E5 または同等のライセンスがあることを確認
- □ macOS デバイスモニタリングがオンで、少なくとも 1 台の Mac が Purview で Updated 状態
- □ Windows デバイスモニタリングがオン（保護対象の Windows デバイスが eSolia にある場合）
- □ Advanced Audit の取り込みが有効
- □ Pay-as-you-go billing リンクが設定済み（または現在のスコープでは不要と判明）
- □ 7 層ラベル分類体系が存在し、EN と JA 両方の名前がセットされ、Confidential と Restricted に暗号化が設定済み
- □ ラベルポリシーが 7 つのラベルを全ユーザーに公開
- □ 5 つの Entra ID セキュリティグループ（Bypass-Documentation、Finance-Exception、Legal-Exception、Departing-Employees、MNPI-Authorized）が作成済み
- □ 普段使いと別のテストユーザーアカウントを保有

- □ Defender for Endpoint が健全で DLP が active な Mac にアクセスできる

すべてチェックが付いたら、フェーズ 1 へ進む。

フェーズ 1：ベースラインルールを audit mode で展開

ゴール：すべてのルールをユーザー通知なしの audit mode で展開する。Activity Explorer で 14 日間マッチを観察する。フェーズ 1 の終わりは、各ルールが自分のテストコンテンツで適切に発火することを検証し、通知をオンにする前に対処すべき false positive と例外ケースのリストができたとき。

所要時間の目安：初回展開で 60〜75 分。

Step 1.1: クラウド認証情報の保護ルール

Purview ポータル → Solutions → Data Loss Prevention → Policies → **Create policy**。

- **Category:** Custom
- **Template:** Custom policy
- **Name:** `eSolia Baseline - Cloud Credential Protection`
- **Description:**「API キー、SSH キー、接続文字列、クラウド認証情報を検出します。メール、SharePoint、OneDrive、Teams、エンドポイントアクション経由での認証シークレットの誤共有を防ぎます。」
- **Admin units:** None（テナント全体に適用）
- **Locations:** ON にする：Exchange email、SharePoint sites、OneDrive accounts、Teams chat and channel messages、Devices。それ以外はオフのまま。
- **Define policy settings:** Create or customize advanced DLP rules
- **「Next」をクリックしてルールエディタへ進み、「Create rule」**

ルールエディタで：

- **Name:** `Detect cloud credentials`
- **Conditions → Add condition → Content contains → Add → Sensitive info types**
- 以下すべてを追加（各項目をクリックしてルールに追加）：
  - `Azure Storage Account Key`
  - `Azure Storage Account Key (Generic)`
  - `Azure Service Bus Connection String`
  - `Azure IoT Connection String`
  - `Azure SQL Connection String`
  - `Azure DocumentDB Auth Key`
  - `Azure Publish Setting Password`
  - `Amazon S3 Client Secret Access Key`
  - `Amazon AWS Access Key ID`
  - `Google API Key`
  - `JSON Web Token`
  - `SSH Private Key`
  - `General Password`
- **Confidence level:** Medium（デフォルト）
- **Instance count:** 1 to Any
- **Actions → Add an action:**
  - **Restrict access or encrypt the content in Microsoft 365 locations** → デフォルトのまま（audit mode では制限なし）

    - **Audit or restrict activities on devices** → 展開して以下を有効化：Upload to a restricted cloud service domain or access from an unallowed browser、Copy to clipboard、Copy to a USB removable device。それぞれ **Audit only** に設定。
- **User notifications:** フェーズ 1 では OFF
- **User overrides:** フェーズ 1 では OFF
- **Incident reports:** テスト管理者メールに高優先度で送信。「Choose what to include in the report」をクリックしてすべてチェック。
- **Additional options → Rule priority:** 0（最高）
- **ルールを保存**

ポリシーエディタに戻って：

- **Set policy mode:** Run the policy in test mode → 「Show policy tips while in test mode」OFF（フェーズ1 では通知なし）
- **Submit and review → Submit**

ポリシーが Policies リストに「Test (without notifications)」のステータスで表示されます。これが audit-only に相当します。

Step 1.2: Sensitivity label enforcement ルール

同じポリシー作成フロー。

- **Name:** `eSolia Baseline - Sensitivity Label Enforcement`
- **Description:** 「eSolia sensitivity label が付与されたコンテンツの取り扱いルールを enforce します。Protected Internal、Client Confidential、Confidential、Restricted のコンテンツを不適切な共有や移動から保護します。」
- **Locations:** Exchange email、SharePoint sites、OneDrive accounts、Teams chat and channel messages、Devices
- **ルールエディタ → Create rule:**
    - **Name:** `Protected Internal label - block external sharing`
    - **Conditions:** Content contains → Sensitivity labels → `Protected Internal / 社内一般`（eSolia-ProtectedInternal）
    - **Conditions → Add group → AND** → Content is shared from Microsoft 365 → with people outside my organization
    - **Actions:** Restrict access (Microsoft 365 locations) → 組織外のユーザーのみブロック。Audit/restrict on devices → Upload to cloud service: Audit only。
    - **User notifications/overrides/reports:** Step 1.1 と同じ（フェーズ 1 ではオフ、incident reports はオン）
    - **ルールを保存**

同じポリシーに 2 つ目のルールを追加：

- **Add rule** → 「Confidential label - tighter restrictions」
- **Conditions:** Content contains → Sensitivity labels → `Confidential / 機密`（eSolia-Confidential）
- **Actions:** 外部共有をブロック（M365）、デバイスで Audit：Upload to cloud + Copy to USB + Copy to clipboard + Print
- **Save**

同じポリシーに 3 つ目のルールを追加：

- **Add rule** → 「Client Confidential - protect client data」
- **Conditions:** Content contains → Sensitivity labels → `Client Confidential / 顧客機密情報`（eSolia-ClientConfidential）
- **Actions:** 外部共有をブロック（M365）、デバイスで Audit：Upload to cloud + Copy to USB + Print
- **Save**

同じポリシーに 4 つ目のルールを追加：

- **Add rule** → 「Restricted - maximum protection」
- **Conditions:** Content contains → Sensitivity labels → `Restricted / 極秘`（eSolia-Restricted）
- **Actions:** 外部共有をブロック（M365）、デバイスで Audit：Upload to cloud + Copy to USB + Copy to clipboard + Print + Copy to network share + Access by unallowed apps
- **Save**

ポリシーモードを Test without notifications に設定し、submit。

Step 1.3: 日本の個人情報保護ルール

- **Name:** `eSolia Baseline - Japanese Personal Data Protection`
- **Description:**「Japan My Number、住民票コード、パスポート番号、運転免許番号を検出します。APPI コンプライアンスに必須。」
- **Locations:** Exchange、SharePoint、OneDrive、Teams、Devices
- **Rule:**
  - **Name:** `Detect Japan personal identifiers`
  - **Conditions:** Content contains → Sensitive info types →
    - `Japan My Number (Individual Number)`
    - `Japan Resident Registration Number`
    - `Japan Passport Number`
    - `Japan Driver's License Number`
  - **Confidence level:** High（厳しいバリアントを使用 — これらの SIT には false positive が多めの低信頼度バリアントもある）
  - **Instance count:** 1 to Any
  - **Actions:** 外部共有ブロック、デバイスで Audit：Copy to USB + Upload to cloud + Print
  - **User notifications:** OFF（フェーズ 1）
  - **Incident reports:** ON、高優先度、コンプライアンス配信リスト宛
  - **Rule priority:** 0
- **Test without notifications モードで submit**

Step 1.4: 金融データ保護ルール

- **Name:** `eSolia Baseline - Financial Data Protection`
- **Description:**「クレジットカード番号、銀行口座番号、決済認証情報を検出します。」
- **Locations:** Exchange、SharePoint、OneDrive、Teams、Devices
- **Rule:**
  - **Name:** `Detect financial data`
  - **Conditions:** Content contains → Sensitive info types →
    - `Credit Card Number`
    - `Japan Bank Account Number`

    - `International Banking Account Number (IBAN)`
    - `SWIFT Code`
  - **Confidence level:** Medium
  - **Instance count:** 1 to Any
  - **Actions:** 外部共有ブロック、USB コピーとクラウドアップロードを Audit
  - **Rule priority:** 1
- **Test without notifications モードで submit**

Step 1.5: 外部共有制御

サイト固有の Restricted ポリシーは今は飛ばします。eSolia にはまだ Restricted SharePoint サイトのキュレーションリストがありません。これはフェーズ 2 でリストを特定してから追加します。

今は、テナント全体の軽量な外部共有 audit を展開：

- **Name:** `eSolia Baseline - External Sharing Audit`
- **Description:**「コンテンツベースの DLP ルールのバックストップとして、SharePoint と OneDrive コンテンツの全外部共有を audit します。」
- **Locations:** SharePoint sites、OneDrive accounts のみ
- **Rule:**
  - **Name:** `Audit external sharing`
  - **Conditions:** Content is shared from Microsoft 365 → with people outside my organization
  - **Actions:** なし（audit only — 条件マッチ時にアクティビティが自動でログ記録される）
  - **Incident reports:** OFF（ボリュームが大きすぎる）
- **Test without notifications モードで submit**

これは、ベースラインルールの中で恒久的に audit-only のままになる唯一のルールです。仕事は forensic であって preventive ではありません。

Step 1.6: コンサルティングオーバーレイルールの展開

フェーズ 1（audit mode）を続けます。これらのルールはベースラインと並んで audit mode でテナントに追加されます。

1.6a: 複数クライアントドメインの検出

これにはまず keyword dictionary とカスタム SIT のセットアップが必要です。

Keyword dictionary を作成：

1. Purview → Solutions → Data Classification → Classifiers → **Keyword dictionaries** タブ → Create
2. **Name:** `eSolia Client Names and Domains`
3. **Description:**「アクティブなクライアント法人名と主要メールドメイン。CRM から四半期ごとにメンテナンス。」
4. **Source:** ファイルアップロード。ファイルは **UTF-16 LE エンコード** のテキスト、1 行 1 ターム。準備：

```
# macOS/Linux で UTF-8 から UTF-16 LE に変換
iconv -f UTF-8 -t UTF-16LE clients.txt > clients-utf16.txt
```

5. **初期投入：**CRM またはクライアント案件管理ツールから取得。アクティブなクライアントごとに以下を含める：

- クライアントの法人名（英語）

- クライアントの法人名（日本語、株式会社/有限会社などの形式を含む）
- 主要メールドメイン（例：`clientco.co.jp`）
- 関連する子会社名

6. 保存して、dictionary が ready になるまで 5〜10 分待つ。

カスタム SIT を作成：

1. Purview → Solutions → Data Classification → **Sensitive info types** タブ → Create sensitive info type
2. **Name:** `eSolia Multiple Client Identifiers`
3. **Description:**「複数の eSolia クライアント識別子を含むドキュメントを検出します。クライアントデータの混在や案件をまたいだ誤った汚染を捕捉するために使用。」
4. **Patterns → Create pattern:**

- **Confidence level:** Medium
- **Primary element → Add → Keyword dictionary** → `eSolia Client Names and Domains` を選択
- **Character proximity:** 300（デフォルト）
- **Match accuracy and occurrences:**
  - **Minimum count:** 10
  - **Maximum count:** Any

5. 保存し、SIT が ready になるまで待つ（インデックス作成に最大 30 分かかる場合あり）。

ポリシーで使う前に SIT をテスト：

1. SIT 詳細ページから **Test** をクリック → dictionary 内のさまざまなクライアント名に 12〜15 回言及するサンプル文書をアップロード
2. 期待される信頼度レベルでマッチすることを確認
3. クライアント名の言及が 3〜4 個だけのサンプル文書を試して、マッチ**しない**ことを確認
4. マッチが正しくない場合は、threshold または proximity を調整して再テスト

DLP ポリシーを作成：

- **Name:** `eSolia Consulting - Multi-Client Contamination Detection`
- **Description:**「複数の eSolia クライアントの識別子を含むドキュメントを検出します。案件をまたいだ誤データ混入を捕捉。」
- **Locations:** SharePoint、OneDrive、Exchange、Devices
- **Rule:**
  - **Name:** `Detect multiple client mentions`
  - **Conditions:** Content contains → Sensitive info types → `eSolia Multiple Client Identifiers`
  - **Actions:** 外部共有を Audit（フェーズ 1）、クラウドアップロードを Audit、USB コピーを Audit
  - **Rule priority:** 5
- **Test without notifications モードで submit**

1.6b: 案件テンプレートのフィンガープリント
フィンガープリント可能な標準化された案件テンプレートが現在ない場合は飛ばしてください。ある場合は（SOW テンプレート、デリバラブルテンプレート、請求書テンプレート）、進めます：

1. Purview → Data Classification → Classifiers → **Document fingerprints** タブ → Create
2. **Name:** `eSolia SOW Template`

3. **Description:** 「eSolia 標準の SOW テンプレート。このテンプレートから派生したドキュメントは、外部共有前に必ず sensitivity label が付与されているべき。」
4. **Upload file:** SOW テンプレートのクリーンなブランク版をアップロード（クライアントデータなし、プロジェクト固有の内容なし、構造的なフォームのみ）
5. 保存。フィンガープリント化したいテンプレートごとに繰り返す。

それから、それらを参照する DLP ポリシーを作成：

- **Name:** `eSolia Consulting - Engagement Template Tracking`
- **Locations:** SharePoint、OneDrive、Exchange、Devices
- **Rule:**
  - **Name:** `Detect engagement template usage`
  - **Conditions:** Content contains → Add → Document fingerprints → 自分のテンプレート fingerprints を選択
  - **AND NOT**（NOT ロジックで 2 つ目の条件グループを追加）→ Content has sensitivity label = Protected Internal、Client Confidential、Confidential、または Restricted
  - **Actions:** フェーズ 1 では Audit のみ（フェーズ 2 で Notify に切り替えて、ユーザーにこれらのドキュメントへのラベル付与を促す）
- **Test without notifications モードで submit**

1.6c: ソースコード検出

- **Name:** `eSolia Consulting - Source Code Detection`
- **Description:** 「メールと Teams メッセージ内のソースコードを検出します。ソースコードはチャットではなく git を通すべき。」
- **Locations:** Exchange、Teams、Devices
- **Rule:**
  - **Name:** `Detect source code in messages`
  - **Conditions:** Content contains → Trainable classifiers → `Source Code`
  - **Actions:** 外部共有（メール）を Audit、クラウドアップロード（デバイス）を Audit
- **Test without notifications モードで submit**

1.6d: Information barriers

eSolia では飛ばす。 Information barriers は、同じスタッフ上で競合するクライアント案件が同時並行で動いている場合にのみ必要です。eSolia の現状の案件モデルでは不要であり、barrier 展開の disruption を正当化できません。フェーズ 4 のレビューで状況が変わったか確認することを文書化しておきます。

Step 1.7: 選択した SMB 項目の展開

1.7a: 退職予定者監視

これは DLP ではなく Insider Risk Management でセットアップします。

1. Purview → Solutions → **Insider Risk Management**
2. 初回セットアップ :まだ完了していない場合は Settings ウィザードを完了する（Privacy settings、Policy timeframes、Intelligent detections、Export alerts、Priority user groups、Power Automate flows、Inline alert customization）。eSolia の規模では：

- **Privacy:** ユーザー名を表示（匿名化しない）— 小組織なので匿名化は非実用的
- **Policy timeframes:** Activation window 30 日、past activity 30 日
- **Alert volume:** デフォルト

3. Policies → **Create policy** → Template: **Data leaks by priority users**

4. ユーザーとグループを選択 → グループを選択：`eSolia-Departing-Employees`
5. 指標を設定：Office indicators（ファイルアクティビティ）、Device indicators（USB 使用、ファイルアクティビティ、Web ブラウジング）、Network indicators（クラウドアクティビティ）を有効化
6. 検出：当面はデフォルト閾値を使用
7. Name: `eSolia - Departing Employee Activity Monitoring`
8. 保存

ポリシーは武装されましたが、`eSolia-Departing-Employees` グループに誰かが入らない限り発火しません。**重要な運用依存：** HR の offboarding チェックリストに「退職通知の日付に、従業員を `eSolia-Departing-Employees` グループに追加する」を含める必要があります。これがないとポリシーは無意味です。

1.7b: 標準デバイス制御
すでにステップ 1.2 の Sensitivity Label Enforcement ポリシーでカバー済み — Confidential と Restricted ルールにデバイス制御アクションが含まれます。eSolia の規模では別ポリシー不要。

フェーズ 1 サインオフチェックリスト

展開後、以下を確認：

- □ 全 8 ポリシーが Purview → Data Loss Prevention → Policies に「Test (without notifications)」モードで表示されている
- □ Departing Employees グループを対象とする Insider Risk Management ポリシーが少なくとも 1 つ存在
- □ 各ポリシーの「Policy sync status」が、自分の Mac で最近の同期（過去 24 時間以内）を表示
- □ Cloud Credential と Japan Personal Data アラートを受信するベースラインのインシデント受信箱を準備済み

それから、フェーズ 2 に進む前に **14 日間待つ**。この期間に以下を行います：

- **各ルールを合成データでテスト**（実際のクライアントデータは使わない）：
  - クラウド認証情報：偽物の AWS キーを Word 文書に貼り付けて保存し、Activity Explorer を確認
  - Japan My Number：Microsoft ドキュメントのテスト番号をテストドキュメントで使用
  - Sensitivity labels：各ラベルをテストドキュメントに付与し、外部メール送信を試す
  - Multi-client：dictionary から 12 個の架空の「クライアント」名を含む文書を作成
- **Activity Explorer を最初の 3 日間は毎日、その後は 2〜3 日ごとに確認**
- **false positive を追跡シートに文書化**
- **何もマッチしていないルールに注意** — 設定の問題を示している可能性
- **リックまたは別のレビュアーにポリシーリストをスポットチェックしてもらう** ですべてが正しいか確認

フェーズ 2：通知モード

ゴール :すべての enforce mode ルールに対してユーザー通知をオンにする。Block アクションはオフのまま。狙いはユーザー行動の訓練と、例外が必要な正当なユースケースの洗い出し。

所要時間の目安：30 分。

開始前に、以下を準備：

- フェーズ 1 の false positive 追跡シート ー 通知をオンにする前に例外を追加する必要がある
- 何が起きるかを説明するユーザー向けコミュニケーションのドラフト、EN と JA で

Step 2.1: 事前通知のコミュニケーション送信

通知をオンにする数日前に、eSolia 全スタッフにメールまたは Teams で告知を送ります。短く。両言語のサンプルテキストはこのランブックの末尾の Appendix B にあります。

Step 2.2: 各ポリシーを Test から Test+Notifications に更新

以下の各ポリシーに対して：

- `eSolia Baseline - Cloud Credential Protection`
- `eSolia Baseline - Sensitivity Label Enforcement`
- `eSolia Baseline - Japanese Personal Data Protection`
- `eSolia Baseline - Financial Data Protection`
- `eSolia Consulting - Multi-Client Contamination Detection`
- `eSolia Consulting - Source Code Detection`

各ポリシーで：

1. Purview → Data Loss Prevention → Policies → ポリシーをクリック → Edit
2. Policy mode までステップを進める
3.「Run the policy in test mode」から **「Run the policy in test mode and show policy tips」** に変更
4. ルールにステップインしてユーザー通知を有効化：

- **Notify users in Office 365 service with a policy tip:** ON
- **Send the user a notification email:** OFF（in-product のヒントで十分。メールは煩わしい）
- **Customize the policy tip text:** バイリンガルテキストを使用。Cloud Credentials のサンプル： >「This content appears to contain cloud credentials or authentication secrets. Sharing credentials externally is not permitted. このコンテンツにはクラウド認証情報が含まれている可能性があります。認証情報の外部共有は禁止されています。」

5. **User overrides:** ON、business justification を要求、override を許可
6. 保存して再公開

Engagement Template Tracking は飛ばす ー このアクションは informational なので audit-only のまま。

External Sharing Audit は飛ばす ー 恒久的に audit-only。

Step 2.3: 観察と対応

次の 14 日間：

- **ユーザーの質問に素早く対応。**フェーズ 2 後の最初の 48 時間に質問が最も多い。FAQ を準備しておく。

- **Override justification を追跡** — ユーザーが override するとき何を書いているかを読む。これがポリシーチューニングのインサイトの最も豊かな源泉。
- **調整** — 特定のルールが正当な理由で過剰な override を生成している場合、ルールに例外グループまたはスコープ変更が必要というサイン。ブロックではなく。
- **追跡シートを更新** — 新しい false positive やエッジケースで。

フェーズ 2 サインオフチェックリスト

- □ すべてのカスタマー向けルールでユーザー通知テキストがバイリンガル
- □ User overrides が business justification を要求（単なる確認ではない）
- □ 事前通知のコミュニケーションが全スタッフに送信済み
- □ よくある質問に対する FAQ ドキュメントを準備済み
- □ Override justification ログが少なくとも 2 日に 1 回レビューされている

フェーズ 3 に進む前にさらに 14 日待つ。この時間でポリシーと例外を refine する。

フェーズ 3：Enforce モード

ゴール：ベースラインがブロックを要求しているルールでブロックをオンにする。Audit-mode のルールはそのまま。

所要時間の目安：30 分プラスユーザーへの周知。

Step 3.1: 事前 enforcement のコミュニケーション送信

フェーズ 2 のコミュニケーションと同じチャネルで。指定日から、ブロックされるアクションが通知ではなく実際にブロックされるようになることをユーザーに伝える。期待値を設定：ほとんどのユーザーは何も変化に気づかない。ルールがブロックする行為をしていないから。今日通知を見ているユーザーは明日ブロックされる。

Step 3.2: 各ポリシーを Test から Enforce に更新

以下のポリシー：

- `eSolia Baseline - Cloud Credential Protection`
- `eSolia Baseline - Sensitivity Label Enforcement`
- `eSolia Baseline - Japanese Personal Data Protection`
- `eSolia Baseline - Financial Data Protection`
- `eSolia Consulting - Multi-Client Contamination Detection`

手順：

1. ポリシーを編集 → Policy mode → **「Turn the policy on」**（通知付きの enforce モード）
2. 保存して再公開
3. 同期を待つ（5〜30 分）

Source Code Detection について：さらに 30 日間 test+notifications モードのままにする。ソースコードに対する block mode は通常のコンサルティング作業で friction が大きすぎる。実際に欲しいのは通知だけ。

Engagement Template Tracking について：test（通知なし）から test+notifications に変更。Enforce はしない ー アクションは「ユーザーに文書のラベル付与を促す」ことであり、丁寧なヒントが正しいツール。

External Sharing Audit について：test+no-notifications のまま。永遠に audit only。

Step 3.3: Enforcement が動作していることを確認

保存後 30 分以内に：

1. 管理対象 Mac 上のテストユーザーアカウントから、新規 Word 文書を開く
2. テスト用の AWS access key を貼り付ける（実物ではなく Microsoft ドキュメントの例を使う）
3. 文書を許可リスト外の宛先（例：wetransfer.com）にアップロードしようとする
4. アップロードがブロックされ、ポリシーのヒントを表示する通知が出るはず
5. Activity Explorer を確認 ー テストアクションに対して「Blocked」イベントがあるはず

ブロックが発火しない場合：ポリシーが「Test」ではなく「On」モードであることを確認、テストユーザーがバイパスグループに入っていないことを確認、宛先が許可リストに入っていないことを確認、SIT が貼り付けた内容と実際にマッチしていることを確認。

フェーズ 3 サインオフチェックリスト

- □ すべてのブロッキングルールが「Test」ではなく「On」モード
- □ 検証テストでテストコンテンツに対して実際のブロックが発火することを確認

- □ Activity Explorer がブロックされたイベントを正しく表示
- □ ユーザーへのコミュニケーションが送信され受領されている
- □ 重要なビジネスプロセスが壊れていない（24 時間後にチームリードで確認）

フェーズ 4：定常運用

展開は完了。ここからはメンテナンスとチューニングのループ。

月次タスク

- 過去 1 ヶ月の Activity Explorer をレビュー：マッチタイプ上位、ユーザー上位、ブロックされたアクション上位、override justifications
- Override justification ログをレビュー：ユーザーが同じ理由で繰り返し override しているか？それは恒久的なルール変更にすべき例外。
- ランダムなマッチを 5〜10 件スポットチェックして正しく見えることを確認
- Insider Risk Management アラートをレビュー（誰かが Departing Employees に入っていない限りゼロに近いはず）

四半期タスク

- 現在の CRM/案件リストから `eSolia Client Names and Domains` keyword dictionary をリフレッシュ
- 四半期にリリースされた新しい Microsoft Purview 機能をレビュー ー 適用できるものがあるか確認
- バイパスグループをレビュー：`eSolia-DLP-Bypass-Documentation`、`Finance-Exception`、`Legal-Exception` に正しい人が入っているか
- ラベル採用率をレビュー：何件のドキュメントがラベル付与されているか？利用が少ない場合は auto-labeling ルールを検討。

年次タスク

- ポリシーリファレンスドキュメントに対するベースラインの完全レビュー ー eSolia ベースライン標準で何か変わったか？
- eSolia リーダーシップとの展開計画の再交渉：新しい要件、新しいクライアントタイプ、新しい規制
- 前提条件検証（フェーズ 0）を再監査して何もドリフトしていないことを確認
- 災害復旧テスト：明日 Purview 管理者アクセスを失ったら、リカバリ手順は？

トリガータスク

- **新入社員：** アカウント作成後 24 時間以内に sensitivity labels が Office アプリで受信されることを確認、最初の 1 週間以内にデバイスが Purview にオンボードされることを確認
- **退職予定者：** HR が通知日に `eSolia-Departing-Employees` グループに追加し、最終勤務日に削除
- **新クライアント：** 次回月次更新時にドメインと法人名をクライアント辞書に追加。案件が sensitive ならもっと早く。
- **新サービス提供：** 新しいポリシーが必要かレビュー
- **新クラウドサービスの採用：** allowlist に追加、または適切な場合は明示的に unallowlist に追加
- **Microsoft ポリシーリファレンス文書の更新：** 展開済みポリシーへの変更をレビューして適用

Appendix A: 検証用テストデータ

フェーズ 1 とフェーズ 3 の検証テストには以下のソースを使用してください。テストに実際のクライアントデータを絶対に使わないこと。

- **クラウド認証情報：** Microsoft ドキュメントが https://learn.microsoft.com/en-us/purview/sit-defn-azure-storage-account-key-generic などのページにサンプルキーを提供しています。SIT にマッチする認識可能なテストパターンです。
- **Japan My Number：** 公式テスト番号 `123456789018` を使用（チェックデジットを満たすが reserved として実在しないと文書化されたテストパターン）
- **クレジットカード：** `4111-1111-1111-1111` は標準の PCI-DSS テスト番号（Visa）。Luhn 有効。
- **Sensitivity labels：** 自分が作成・所有するテストドキュメントに自分の eSolia ラベルを付与。実際のドキュメントを relabel しない。
- **Multi-client SIT：** dictionary のテスト版に追加した 12 個の架空の「クライアント」名を含む偽ドキュメントを作成。

Appendix B: ユーザーコミュニケーションテンプレート

フェーズ 2 告知（English）

> Subject: New protection for sensitive content in our M365 environment
>
> Starting [date], you may begin seeing notifications when you handle certain types of sensitive content in Word, Outlook, Teams, and other Microsoft 365 apps. These notifications are part of new data loss prevention rules that protect cloud credentials, Japanese personal data, financial information, and content marked with eSolia sensitivity labels.
>
> For the first two weeks, the rules will only notify you — nothing will be blocked. The notification will explain what was detected and how to proceed. If you have a legitimate business reason to continue, you'll be able to override with a brief justification.
>
> If you have questions or see notifications you don't understand, contact [support contact]. We'd rather hear about confusion now than after blocking starts.

フェーズ 2 告知（日本語）

> 件名：M365 環境の機密コンテンツ保護開始のお知らせ
>
> [日付] より、Word、Outlook、Teams、その他の Microsoft 365 アプリで特定の種類の機密コンテンツを扱う際に、通知が表示される場合があります。これは、クラウド認証情報、日本の個人情報、金融情報、eSolia の機密ラベルが付与されたコンテンツを保護する新しいデータ損失防止ルールの一部です。
>
> 最初の 2 週間は、ルールは通知のみで、何もブロックしません。通知には何が検出されたか、どう進めればよいかが表示されます。正当なビジネス理由がある場合は、簡単な justification を入力して override できます。
>
> 質問や、理解できない通知があった場合は、[サポート連絡先] までご連絡ください。ブロック開始後よりも、今のうちに混乱を解消したいです。

フェーズ 3 告知（English）

> Subject: Reminder: data loss prevention rules begin enforcing on [date]
>
> A reminder that starting [date], the data loss prevention rules you've been seeing notifications about will begin actively blocking the actions they detect, instead of just notifying.
>
> Most users will see no change. The rules block: sharing cloud credentials externally, sharing Japan My Number externally, sharing credit card numbers externally, sharing content marked with Confidential or Restricted labels externally, and a few other narrowly-defined situations.

> If you legitimately need to perform an action the rules block, contact [support contact] for an exception or use the in-product override option where available. Most blocks include an override option with business justification.
>
> Thanks for your patience during the rollout.

フェーズ 3 告知（日本語）

> 件名：リマインド：データ損失防止ルールが [日付] より enforce 開始
>
> リマインドです。[日付] より、これまで通知だけだったデータ損失防止ルールが、検出したアクションを実際にブロックするようになります。
>
> ほとんどのユーザーにとって変化はありません。ルールがブロックするのは：クラウド認証情報の外部共有、Japan My Number の外部共有、クレジットカード番号の外部共有、Confidential または Restricted ラベルが付与されたコンテンツの外部共有、その他いくつかの限定的な状況です。
>
> ルールがブロックするアクションを正当に実行する必要がある場合は、[サポート連絡先] まで例外申請してください。または、利用可能な場合はアプリ内の override オプション（business justification 入力）を使用してください。
>
> 展開期間中のご協力ありがとうございます。

Appendix C: クイックリファレンスシーケンス

繰り返し使用または同僚への引き継ぎ用：

```
Day 0:    フェーズ0 検証（15〜20分）
          フェーズ1 全8ポリシーを test mode で展開（60〜75分）
Days 1-3: Activity Explorer を毎日確認
Day 7:    中間レビュー、false positive を文書化
Day 14:   フェーズ2 移行（30分）+ ユーザー告知
Days 15-28: ユーザーの質問対応、override を追跡
Day 28:   フェーズ3 移行（30分）+ ユーザー告知
Day 29:   Enforce mode の検証テスト
Day 30+:  定常運用 - 月次/四半期/年次サイクル
```

お問い合わせ

株式会社イソリア 〒105-7105 東京都港区東新橋 1-5-2 汐留シティセンター 5 階 (Workstyling)

電話	03-4577-3380
メール	hello@esolia.co.jp
Web	https://esolia.co.jp
営業時間	月～金、9:00～18:00

eSolia

Purview DLP Setup Runbook

April 11, 2026

Contents

> eSolia INTERNAL — Not for distribution outside eSolia

A step-by-step runbook for deploying Microsoft Purview Data Loss Prevention to eSolia's own tenant. Covers prerequisite verification, the full eSolia baseline (5 rules), the consulting overlay (4 additions), and selected SMB items (departing employee monitoring, light-touch device controls). Plan for 6-10 hours of total work spread over 4-6 weeks of phased rollout.

Before you start

This runbook is the "how" companion to `eSolia-Purview-DLP-Baseline-Policy-Reference-INTERNAL-20260411-en.md`, which is the "what and why." Read the reference first for background on each policy. This document focuses on click paths, exact configuration values, and the order of operations specific to eSolia's tenant.

You'll need:

- **An admin account with Compliance Administrator and Security Administrator roles**, activated through PIM if applicable
- **A working session at the Microsoft Purview portal** (`https://purview.microsoft.com`) with eSolia tenant context confirmed (`tid=436f19ac-627e-4ec1-bfcb-7404d06a5b46` in the URL)
- **PowerShell on a machine with Microsoft Graph and ExchangeOnlineManagement modules installed**, for the prerequisite verification steps
- **About 90 minutes for the initial deployment session**, then check-in time over the following weeks for phase transitions and tuning
- **A test user account** that is not your daily account, for verification testing without polluting your own audit trail

A reasonable rollout schedule: do the prereq verification and Phase 1 (audit mode) on day 1 (90 minutes). Watch Activity Explorer for two weeks. Do Phase 2 (notify mode) on day 14 (30 minutes). Watch and answer questions for two more weeks. Do Phase 3 (enforce) on day 28 (30 minutes plus user communication). Steady state from there.

Phase 0: Prerequisite verification

Don't skip this. Most failed Purview deployments fail because someone assumed a prerequisite was in place that wasn't. The verification takes 15-20 minutes and saves hours of debugging.

Step 0.1: Confirm licensing

```
Connect-MgGraph -Scopes "Organization.Read.All","Directory.Read.All"
Get-MgSubscribedSku | Select SkuPartNumber, ConsumedUnits,
@{N='Enabled';E={$_.PrepaidUnits.Enabled}}
```

You should see at least one of:

- `SPE_E5` (Microsoft 365 E5)
- `INFORMATION_PROTECTION_COMPLIANCE` (M365 E5 Compliance add-on)
- `M365_E5_INFO_PROTECTION_GOVERNANCE` (M365 E5 IP&G add-on)

If none are present or the count is zero, stop. The baseline assumes E5-level Information Protection capabilities. Without them, you can deploy a subset (basic SITs, manual sensitivity labels, basic DLP) but you lose endpoint DLP, trainable classifiers, auto-labeling, and Insider Risk Management — most of what makes the baseline valuable.

For eSolia specifically: as of 2026, Rick and select admin/IT users should have E5; the rest of staff have E3. This is fine for the baseline because the baseline policies apply to the tenant, not per-user. End users need to be licensed for whatever features touch them: sensitivity labels (E3 sufficient for manual application, E5 for auto-labeling), endpoint DLP (E5), and so on. Document any per-user licensing constraints so you don't deploy a policy that fails silently for E3 users.

Step 0.2: Confirm Endpoint DLP device monitoring is on

In the Purview portal:

1. Settings (gear icon, top right) → Device onboarding → Devices
2. Confirm both **"Turn off Windows device monitoring"** and **"Turn off macOS device monitoring"** appear (the inverse phrasing means monitoring is currently on; if the button says "Turn on…", it's off)
3. If macOS monitoring is off, click **"Turn on macOS device monitoring"** and wait up to 30 minutes for activation
4. Verify your own Mac (`ESO-LYXN42490K` or current device name) appears in the device list with Configuration status = Updated and Endpoint DLP status = Enabled

If your Mac isn't there or isn't healthy, stop and fix that first using `eSolia-Defender-macOS-DLP-Troubleshooting-Runbook-INTERNAL-20260410-en.md`. You can technically deploy DLP policies before all devices are onboarded — they'll just apply to whatever subset is reporting — but you want to validate against at least one healthy device before flipping anything to enforce.

Step 0.3: Confirm Advanced Audit is enabled

```
Connect-ExchangeOnline
Get-AdminAuditLogConfig | Select UnifiedAuditLogIngestionEnabled
```

Should return `True`. If `False`, enable it:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

This is a one-liner but takes up to 24 hours to start ingesting events. If it was already on, no action needed.

Step 0.4: Confirm pay-as-you-go billing link (optional but recommended)

In the Purview portal: Settings → DLP → Billing. If a yellow banner says you need to link an Azure subscription, follow the link. eSolia's baseline doesn't strictly require pay-as-you-go for any of the rules below, but newer Purview features (advanced classification, EDM, some automation) will silently no-op without it. Worth setting up before you need it.

Step 0.5: Confirm or create the eSolia label taxonomy

The baseline assumes a 7-tier sensitivity label taxonomy. Check what currently exists:

```
Connect-IPPSSession
Get-Label | Select DisplayName, Identity, ParentLabelDisplayName | Sort DisplayName
```

For eSolia, you should have (or be about to create) the following seven parent labels:

Priority	Label internal name	Display name (EN)	Display name (JA)
0	`eSolia-Public`	Public	社外一般
1	`eSolia-WorkShare`	Work Share	業務共有
2	`eSolia-CommercialPapers`	Commercial Papers	商用書類
3	`eSolia-ProtectedInternal`	Protected Internal	社内一般
4	`eSolia-ClientConfidential`	Client Confidential	顧客機密情報
5	`eSolia-Confidential`	Confidential	秘密
6	`eSolia-Restricted`	Restricted	極秘

If these don't exist, create them via Purview portal → Solutions → Information Protection → Labels → Create a label. For each label, configure:

- **Both EN and JA display names** (the Japanese name appears for users with Japanese-language Office)
- **Tooltip** in both languages explaining when to apply
- **Encryption settings** for Confidential and Restricted (Microsoft-managed key, encrypt for "All users in your organization" by default)
- **Content marking** for Restricted: header text "Restricted / 極秘 — eSolia INTERNAL"
- **Endpoint data protection** (this is the key bit that connects labels to DLP rules)

- **Auto-labeling for files and emails** — leave off initially, you'll enable it after the labels are published

Then publish via Purview portal → Solutions → Information Protection → **Label policies** → Create policy. Publish all seven labels to all users, set `eSolia-ProtectedInternal` as the default for new documents, and require justification when downgrading a label.

> **Important:** The 7-tier taxonomy above has been documented in the eSolia Standards MCP. This document references the authoritative version. If the taxonomy is updated in the Standards MCP, update this runbook to match.

Step 0.6: Create supporting Entra ID groups

The runbook references several security groups. Create these in Entra ID before starting Phase 1, all as **assigned** (not dynamic) groups, **security** type:

- `eSolia-DLP-Bypass-Documentation` — users who need to author documentation containing example credentials. Add the Marketing/Content team and yourself.
- `eSolia-DLP-Finance-Exception` — users who legitimately handle financial data internally. Add Accounting/Finance staff.
- `eSolia-DLP-Legal-Exception` — users who legitimately handle contract templates and legal documents. Add anyone with legal review responsibilities.
- `eSolia-Departing-Employees` — empty for now. HR populates this when notice is given. Document in HR's offboarding checklist.
- `eSolia-MNPI-Authorized` — empty for now. eSolia probably doesn't handle MNPI directly, but the group should exist for future use.

Document each group's purpose in its description field so future admins know why it exists.

Phase 0 sign-off checklist

Before proceeding to Phase 1, verify all of the following:

- □ E5 or equivalent licensing confirmed for at least admin users
- □ macOS device monitoring is on and at least one Mac shows Updated status in Purview
- □ Windows device monitoring is on (if eSolia has any Windows devices to protect)
- □ Advanced Audit ingestion is enabled
- □ Pay-as-you-go billing link configured (or known not to be needed for current scope)
- □ 7-tier label taxonomy exists, both EN and JA names set, encryption configured on Confidential and Restricted
- □ Label policy publishes all seven labels to all users
- □ Five Entra ID security groups created (Bypass-Documentation, Finance-Exception, Legal-Exception, Departing-Employees, MNPI-Authorized)
- □ You have a test user account distinct from your daily account
- □ You have access to your Mac with Defender for Endpoint healthy and DLP active

When all boxes are ticked, proceed to Phase 1.

Phase 1: Deploy baseline rules in audit mode

Goal: deploy all rules in audit-only mode with no user notifications. Watch Activity Explorer for matches over 14 days. The end of Phase 1 is when you've validated that each rule fires appropriately on your own test content and you have a list of any false positives or exception cases that need handling before notifications go on.

Estimated time: 60-75 minutes for the initial deployment.

Step 1.1: Cloud credential protection rule

Purview portal → Solutions → Data Loss Prevention → Policies → **Create policy**.

- **Category:** Custom
- **Template:** Custom policy
- **Name:** `eSolia Baseline - Cloud Credential Protection`
- **Description:** "Detects API keys, SSH keys, connection strings, and cloud credentials. Prevents accidental sharing of authentication secrets via email, SharePoint, OneDrive, Teams, and endpoint actions."
- **Admin units:** None (apply to entire tenant)
- **Locations:** Toggle ON: Exchange email, SharePoint sites, OneDrive accounts, Teams chat and channel messages, Devices. Leave others off.
- **Define policy settings:** Create or customize advanced DLP rules
- **Click "Next" through to the rule editor, then "Create rule"**

In the rule editor:

- **Name:** `Detect cloud credentials`
- **Conditions → Add condition → Content contains → Add → Sensitive info types**
- Add all of these (click each one to add to the rule):
  - `Azure Storage Account Key`
  - `Azure Storage Account Key (Generic)`
  - `Azure Service Bus Connection String`
  - `Azure IoT Connection String`
  - `Azure SQL Connection String`
  - `Azure DocumentDB Auth Key`
  - `Azure Publish Setting Password`
  - `Amazon S3 Client Secret Access Key`
  - `Amazon AWS Access Key ID`
  - `Google API Key`
  - `JSON Web Token`
  - `SSH Private Key`
  - `General Password`
- **Confidence level:** Medium (default)
- **Instance count:** 1 to Any
- **Actions → Add an action:**

    - **Restrict access or encrypt the content in Microsoft 365 locations** → leave default (no restriction in audit mode)
    - **Audit or restrict activities on devices** → expand and enable for: Upload to a restricted cloud service domain or access from an unallowed browser, Copy to clipboard, Copy to a USB removable device. Set each to **Audit only** for now.
- **User notifications:** OFF for Phase 1
- **User overrides:** OFF for Phase 1
- **Incident reports:** Send notification to your test admin email at high priority. Click "Choose what to include in the report" and check everything.
- **Additional options → Rule priority:** 0 (highest)
- **Save the rule**

Back in the policy editor:

- **Set policy mode:** Run the policy in test mode → "Show policy tips while in test mode" OFF (we don't want notifications in Phase 1)
- **Submit and review → Submit**

The policy will appear in the Policies list with status "Test (without notifications)" — that's the equivalent of audit-only.

Step 1.2: Sensitivity label enforcement rule

Same policy creation flow.

- **Name:** `eSolia Baseline - Sensitivity Label Enforcement`
- **Description:** "Enforces handling rules for content marked with eSolia sensitivity labels. Protects Protected Internal, Client Confidential, Confidential, and Restricted content from inappropriate sharing or movement."
- **Locations:** Exchange email, SharePoint sites, OneDrive accounts, Teams chat and channel messages, Devices
- **Rule editor → Create rule:**
    - **Name:** `Protected Internal label - block external sharing`
    - **Conditions:** Content contains → Sensitivity labels → `Protected Internal / 社内一般` (eSolia-ProtectedInternal)
    - **Conditions → Add group → AND** → Content is shared from Microsoft 365 → with people outside my organization
    - **Actions:** Restrict access (Microsoft 365 locations) → Block only people outside your organization. Audit/restrict on devices → Upload to cloud service: Audit only.
    - **User notifications/overrides/reports:** Same as Step 1.1 (off for Phase 1, incident reports on)
    - **Save the rule**

Add a second rule to the same policy:

- **Add rule** → "Confidential label - tighter restrictions"
- **Conditions:** Content contains → Sensitivity labels → `Confidential / 機密` (eSolia-Confidential)
- **Actions:** Block external sharing (M365), Audit on devices: Upload to cloud + Copy to USB + Copy to clipboard + Print
- **Save**

Add a third rule:

- **Add rule** → "Client Confidential - protect client data"
- **Conditions:** Content contains → Sensitivity labels → `Client Confidential / 顧客機密情報` (eSolia-ClientConfidential)
- **Actions:** Block external sharing (M365), Audit on devices: Upload to cloud + Copy to USB + Print
- **Save**

Add a fourth rule:

- **Add rule** → "Restricted - maximum protection"
- **Conditions:** Content contains → Sensitivity labels → `Restricted / 極秘` (eSolia-Restricted)
- **Actions:** Block external sharing (M365), Audit on devices: Upload to cloud + Copy to USB + Copy to clipboard + Print + Copy to network share + Access by unallowed apps
- **Save**

Set policy mode to Test without notifications, submit.

Step 1.3: Japanese personal data protection rule

- **Name:** `eSolia Baseline - Japanese Personal Data Protection`
- **Description:** "Detects Japan My Number, resident registration numbers, passport numbers, and driver's license numbers. Required for APPI compliance."
- **Locations:** Exchange, SharePoint, OneDrive, Teams, Devices
- **Rule:**
  - **Name:** `Detect Japan personal identifiers`
  - **Conditions:** Content contains → Sensitive info types →
    - `Japan My Number (Individual Number)`
    - `Japan Resident Registration Number`
    - `Japan Passport Number`
    - `Japan Driver's License Number`
  - **Confidence level:** High (use the strict variant — these SITs have lower-confidence variants that produce more false positives)
  - **Instance count:** 1 to Any
  - **Actions:** Block external sharing, Audit on devices: Copy to USB + Upload to cloud + Print
  - **User notifications:** OFF (Phase 1)
  - **Incident reports:** ON, high priority, to compliance distribution list
  - **Rule priority:** 0
- **Submit in Test without notifications mode**

Step 1.4: Financial data protection rule

- **Name:** `eSolia Baseline - Financial Data Protection`
- **Description:** "Detects credit card numbers, bank account numbers, and payment credentials."
- **Locations:** Exchange, SharePoint, OneDrive, Teams, Devices
- **Rule:**
  - **Name:** `Detect financial data`
  - **Conditions:** Content contains → Sensitive info types →
    - `Credit Card Number`

    - `Japan Bank Account Number`
    - `International Banking Account Number (IBAN)`
    - `SWIFT Code`
  - **Confidence level:** Medium
  - **Instance count:** 1 to Any
  - **Actions:** Block external sharing, Audit USB copy and cloud upload
  - **Rule priority:** 1
- **Submit in Test without notifications mode**

Step 1.5: External sharing controls

Skip the site-specific Restricted policy for now — eSolia doesn't yet have a curated list of Restricted SharePoint sites. We'll add this in Phase 2 once you've identified them.

For now, deploy a tenant-wide light-touch external sharing audit:

- **Name:** `eSolia Baseline - External Sharing Audit`
- **Description:** "Audits all external sharing of SharePoint and OneDrive content as a backstop for content-based DLP rules."
- **Locations:** SharePoint sites, OneDrive accounts (only)
- **Rule:**
  - **Name:** `Audit external sharing`
  - **Conditions:** Content is shared from Microsoft 365 → with people outside my organization
  - **Actions:** None (audit-only — the activity is logged automatically when the condition matches)
  - **Incident reports:** OFF (this would generate too much volume)
- **Submit in Test without notifications mode**

This is the only baseline rule that stays in audit-only permanently. Its job is forensic, not preventive.

Step 1.6: Deploy the consulting overlay rules

Continue in Phase 1 (audit mode) — these rules are added to the tenant in audit mode alongside the baseline.

1.6a: Multi-client domain detection

This requires setting up a keyword dictionary and a custom SIT first.

Create the keyword dictionary:

1. Purview → Solutions → Data Classification → Classifiers → **Keyword dictionaries** tab → Create
2. **Name:** `eSolia Client Names and Domains`
3. **Description:** "Active client legal names and primary email domains. Maintained quarterly from CRM."
4. **Source:** Upload a file. The file must be **UTF-16 LE encoded** text, one term per line. To prepare:

```
# On macOS/Linux, convert from UTF-8 to UTF-16 LE
iconv -f UTF-8 -t UTF-16LE clients.txt > clients-utf16.txt
```

5. **Initial population:** Pull from your CRM or client engagement tracker. Include for each active client:

- Client legal name (English)
- Client legal name (Japanese, including 株式会社/有限会社 forms)

- Primary email domain (e.g., `clientco.co.jp`)
- Common subsidiary names if relevant

6. Save and wait 5-10 minutes for the dictionary to be ready.

Create the custom SIT:

1. Purview → Solutions → Data Classification → **Sensitive info types** tab → Create sensitive info type
2. **Name:** `eSolia Multiple Client Identifiers`
3. **Description:** "Detects documents containing multiple eSolia client identifiers. Used to flag potential client data mixing or accidental cross-engagement contamination."
4. **Patterns → Create pattern:**

- **Confidence level:** Medium
- **Primary element → Add → Keyword dictionary** → select `eSolia Client Names and Domains`
- **Character proximity:** 300 (default)
- **Match accuracy and occurrences:**
  - **Minimum count:** 10
  - **Maximum count:** Any

5. Save and wait for the SIT to be ready (can take up to 30 minutes for indexing).

Test the SIT before using it in a policy:

1. From the SIT detail page, click **Test** → upload a sample document containing 12-15 mentions of various client names from your dictionary
2. Confirm it matches at the expected confidence level
3. Try a sample document with only 3-4 client names and confirm it does NOT match
4. If matching is wrong, adjust the threshold or proximity and re-test

Create the DLP policy:

- **Name:** `eSolia Consulting - Multi-Client Contamination Detection`
- **Description:** "Detects documents containing identifiers from multiple eSolia clients. Catches accidental cross-engagement data mixing."
- **Locations:** SharePoint, OneDrive, Exchange, Devices
- **Rule:**
  - **Name:** `Detect multiple client mentions`
  - **Conditions:** Content contains → Sensitive info types → `eSolia Multiple Client Identifiers`
  - **Actions:** Audit external sharing (Phase 1), Audit cloud upload, Audit USB copy
  - **Rule priority:** 5
- **Submit in Test without notifications mode**

1.6b: Engagement template fingerprinting

Skip this if you don't currently have standardized engagement templates ready to fingerprint. If you do (SOW template, deliverable template, invoice template), proceed:

1. Purview → Data Classification → Classifiers → **Document fingerprints** tab → Create
2. **Name:** `eSolia SOW Template`
3. **Description:** "Standard eSolia statement of work template. Documents derived from this template should always have a sensitivity label applied before external sharing."

4. **Upload file:** Upload a clean blank version of the SOW template (no client data, no project specifics — just the structural form)
5. Save. Repeat for each template you want to fingerprint.

Then create a DLP policy referencing them:

- **Name:** `eSolia Consulting - Engagement Template Tracking`
- **Locations:** SharePoint, OneDrive, Exchange, Devices
- **Rule:**
  - **Name:** `Detect engagement template usage`
  - **Conditions:** Content contains → Add → Document fingerprints → select your template fingerprints
  - **AND NOT** (add a second condition group with NOT logic) → Content has sensitivity label = Protected Internal, Client Confidential, Confidential, or Restricted
  - **Actions:** Audit only in Phase 1 (will flip to Notify in Phase 2 to prompt users to label these documents)
- **Submit in Test without notifications mode**

1.6c: Source code detection

- **Name:** `eSolia Consulting - Source Code Detection`
- **Description:** "Detects source code in emails and Teams messages. Source code should travel through git, not chat."
- **Locations:** Exchange, Teams, Devices
- **Rule:**
  - **Name:** `Detect source code in messages`
  - **Conditions:** Content contains → Trainable classifiers → `Source Code`
  - **Actions:** Audit external sharing (email), Audit cloud upload (devices)
- **Submit in Test without notifications mode**

1.6d: Information barriers

Skip for eSolia. Information barriers are needed only when you have competing-client engagements running simultaneously on the same staff. eSolia's current engagement model doesn't require this, and the disruption of deploying barriers isn't justified. Document in Phase 4 review whether this changes.

Step 1.7: Deploy selected SMB items

1.7a: Departing employee monitoring

This is set up in Insider Risk Management, not DLP.

1. Purview → Solutions → **Insider Risk Management**
2. First-time setup: complete the Settings wizard if you haven't already (Privacy settings, Policy timeframes, Intelligent detections, Export alerts, Priority user groups, Power Automate flows, Inline alert customization). For eSolia's scale:

- **Privacy:** Show usernames (not anonymized) — small org, anonymization is impractical
- **Policy timeframes:** Activation window 30 days, past activity 30 days
- **Alert volume:** Default

3. Policies → **Create policy** → Template: **Data leaks by priority users**
4. Choose users and groups → Select group: `eSolia-Departing-Employees`

5. Configure indicators: enable Office indicators (file activity), Device indicators (USB usage, file activity, web browsing), Network indicators (cloud activity)
6. Detection: Use default thresholds for now
7. Name: `eSolia - Departing Employee Activity Monitoring`
8. Save

The policy is now armed but won't fire unless someone is in the `eSolia-Departing-Employees` group. **Critical operational dependency:** the HR offboarding checklist must include "Add employee to `eSolia-Departing-Employees` group on date of notice." Without this, the policy is useless.

1.7b: Standard device controls

Already covered by the Sensitivity Label Enforcement policy in Step 1.2 — the Confidential and Restricted rules include device control actions. No separate policy needed for eSolia at this scale.

Phase 1 sign-off checklist

After deployment, verify the following:

- □ All 8 policies appear in Purview → Data Loss Prevention → Policies in "Test (without notifications)" mode
- □ At least one Insider Risk Management policy exists targeting Departing Employees group
- □ Each policy's "Policy sync status" shows recent sync (within last 24 hours) for your Mac
- □ You have a baseline incident inbox set up to receive Cloud Credential and Japan Personal Data alerts

Then **wait 14 days** before proceeding to Phase 2. Use this time to:

- **Test each rule with synthetic data** (not real client data):
  - Cloud credentials: paste a fake AWS key into a Word doc, save, watch Activity Explorer
  - Japan My Number: use a test number from Microsoft's documentation in a test document
  - Sensitivity labels: apply each label to a test document and try to email externally
  - Multi-client: create a doc with 12 made-up "client" names from your dictionary
- **Check Activity Explorer daily for the first 3 days, then every 2-3 days**
- **Document any false positives** in a tracking sheet
- **Note any rules that are matching nothing** — that may indicate a configuration issue
- **Get Rick or another reviewer to spot-check the policy list** to confirm everything looks right

Phase 2: Notification mode

Goal: turn on user notifications for all enforce-mode rules. Block actions remain off. The point is to train user behavior and surface legitimate use cases that need exceptions.

Estimated time: 30 minutes.

Before starting, make sure you have:

- A tracking sheet of any false positives from Phase 1 — these need exceptions added before flipping notifications on
- A draft user-facing communication explaining what's happening, in EN and JA

Step 2.1: Send pre-notification communication

Send an email or Teams announcement to all eSolia staff a few days before flipping notifications on. Keep it short. Sample text in both languages is in Appendix B at the end of this runbook.

Step 2.2: Update each policy from Test to Test+Notifications

For each of the following policies:

- `eSolia Baseline - Cloud Credential Protection`
- `eSolia Baseline - Sensitivity Label Enforcement`
- `eSolia Baseline - Japanese Personal Data Protection`
- `eSolia Baseline - Financial Data Protection`
- `eSolia Consulting - Multi-Client Contamination Detection`
- `eSolia Consulting - Source Code Detection`

Process for each:

1. Purview → Data Loss Prevention → Policies → click the policy → Edit
2. Step through to Policy mode
3. Change from "Run the policy in test mode" to **"Run the policy in test mode and show policy tips"**
4. Step into the rule(s) and enable User notifications:

- **Notify users in Office 365 service with a policy tip:** ON
- **Send the user a notification email:** OFF (in-product tip is enough; email is intrusive)
- **Customize the policy tip text:** Use bilingual text. Sample for Cloud Credentials: > "This content appears to contain cloud credentials or authentication secrets. Sharing credentials externally is not permitted. このコンテンツにはクラウド認証情報が含まれている可能性があります。認証情報の外部共有は禁止されています。"

5. **User overrides:** ON, require business justification, allow override
6. Save and republish

Skip Engagement Template Tracking — it stays in audit-only because the action is informational.

Skip External Sharing Audit — it stays in audit-only permanently.

Step 2.3: Watch and respond

Over the next 14 days:

- **Field user questions** promptly. The first 48 hours after Phase 2 will generate the most questions. Have a ready FAQ.
- **Track override justifications** — read what users are saying when they override. This is your richest source of policy tuning insight.
- **Adjust** if a particular rule is generating excessive overrides for a legitimate reason — that's a sign the rule needs an exception group or scope change, not blocking.
- **Update the tracking sheet** with any new false positives or edge cases.

Phase 2 sign-off checklist

- □ User notification text is bilingual on every customer-facing rule
- □ User overrides require business justification (not just acknowledgment)
- □ Pre-notification communication sent to all staff
- □ FAQ document prepared for likely questions
- □ Override justification log being reviewed at least every other day

Wait another 14 days before proceeding to Phase 3. Use the time to refine policies and exceptions.

Phase 3: Enforce mode

Goal: turn on blocking for rules where the baseline calls for blocks. Audit-mode rules stay as they are.

Estimated time: 30 minutes plus user communication.

Step 3.1: Send pre-enforcement communication

Same channel as Phase 2 communication. Inform users that starting on a specific date, blocked actions will actually be blocked rather than notified. Set expectations: most users will see no change because they aren't trying to do the things the rules block. Users who see notifications today will see blocks tomorrow.

Step 3.2: Update each policy from Test to Enforce

For these policies:

- `eSolia Baseline - Cloud Credential Protection`
- `eSolia Baseline - Sensitivity Label Enforcement`
- `eSolia Baseline - Japanese Personal Data Protection`
- `eSolia Baseline - Financial Data Protection`
- `eSolia Consulting - Multi-Client Contamination Detection`

Process:

1. Edit policy → Policy mode → **"Turn the policy on"** (this is the enforce-with-notifications mode)
2. Save and republish
3. Wait for sync (5-30 minutes)

For Source Code Detection: leave in test+notifications mode for another 30 days. Block mode for source code generates too much friction in normal consulting work; the notification is what you actually want.

For Engagement Template Tracking: change from test (no notifications) to test+notifications. Don't enforce — the action is "remind users to label the document," and a polite tip is the right tool.

For External Sharing Audit: leave in test+no-notifications. Audit-only forever.

Step 3.3: Verify enforcement is working

Within 30 minutes of saving:

1. From your test user account on a managed Mac, open a fresh Word doc
2. Paste a test AWS access key (use a Microsoft documentation example, not a real one)
3. Try to upload the doc to a non-allowlisted destination (e.g., wetransfer.com)
4. The upload should be blocked, with a notification showing the policy tip
5. Check Activity Explorer — there should be a "Blocked" event with your test action

If the block doesn't fire: check the policy is in "On" mode and not "Test", check the test user is not in a bypass group, check the destination isn't allowlisted, and confirm the SIT actually matched what you pasted.

Phase 3 sign-off checklist

- □ All blocking rules in "On" mode, not "Test"
- □ Verification test confirms a real block fired against test content
- □ Activity Explorer shows the blocked event correctly

- □ User communication sent and acknowledged
- □ No critical business processes broken (check with team leads after 24 hours)

Phase 4: Steady state operation

The deployment is done; now it's a maintenance and tuning loop.

Monthly tasks

- Review Activity Explorer for the past month: top match types, top users, top blocked actions, override justifications
- Review the override justification log: are users repeatedly overriding for the same reason? That's an exception that should become a permanent rule modification.
- Spot-check 5-10 random matches to confirm they look correct
- Review Insider Risk Management alerts (should be near zero unless someone is in Departing Employees)

Quarterly tasks

- Refresh the `eSolia Client Names and Domains` keyword dictionary from the current CRM/engagement list
- Review any new Microsoft Purview features released in the quarter — see if any apply
- Review the bypass groups: are the right people in `eSolia-DLP-Bypass-Documentation`, `Finance-Exception`, `Legal-Exception`?
- Review label adoption rates: how many documents are getting labeled? If usage is low, consider auto-labeling rules.

Annual tasks

- Full baseline review against the policy reference document — has anything in the eSolia baseline standard changed?
- Renegotiate the deployment plan with eSolia leadership: any new requirements, new client types, new regulations?
- Re-audit the prerequisite verification (Phase 0) to confirm nothing has drifted
- Test disaster recovery: if Purview admin access were lost tomorrow, what's the recovery procedure?

Triggered tasks

- **New employee:** verify they receive sensitivity labels in their Office apps within 24 hours of account creation; verify their device gets onboarded to Purview within their first week
- **Departing employee:** HR adds them to `eSolia-Departing-Employees` group on the day notice is given, removes them on their last day
- **New client:** add their domain and legal name to the client dictionary at the next monthly refresh, or sooner if the engagement is sensitive
- **New service offering:** review whether any new policies are needed
- **New cloud service adoption:** add to the allowlist, or explicitly to the unallowlist if appropriate
- **Microsoft policy reference document update:** review and apply changes to the deployed policies

Appendix A: Test data for verification

Use these sources for Phase 1 and Phase 3 verification testing. Never use real client data for testing.

- **Cloud credentials:** Microsoft documentation provides example keys at https://learn.microsoft.com/en-us/purview/sit-defn-azure-storage-account-key-generic and similar pages. They're recognizable test patterns that match the SITs.
- **Japan My Number:** Use the official test number `123456789018` (this is the documented test pattern that satisfies the check digit but is reserved as non-real)
- **Credit card:** `4111-1111-1111-1111` is the standard PCI-DSS test number (Visa). Luhn-valid.
- **Sensitivity labels:** Apply your own eSolia labels to test docs you create and own; don't relabel real documents.
- **Multi-client SIT:** Create a fake document with 12 made-up "client" names that match entries you've added to a test version of the dictionary.

Appendix B: User communication templates

Phase 2 announcement (English)

> Subject: New protection for sensitive content in our M365 environment
>
> Starting [date], you may begin seeing notifications when you handle certain types of sensitive content in Word, Outlook, Teams, and other Microsoft 365 apps. These notifications are part of new data loss prevention rules that protect cloud credentials, Japanese personal data, financial information, and content marked with eSolia sensitivity labels.
>
> For the first two weeks, the rules will only notify you — nothing will be blocked. The notification will explain what was detected and how to proceed. If you have a legitimate business reason to continue, you'll be able to override with a brief justification.
>
> If you have questions or see notifications you don't understand, contact [support contact]. We'd rather hear about confusion now than after blocking starts.

Phase 2 announcement (Japanese)

> 件名: M365 環境における機密コンテンツ保護の開始
>
> [日付] より、Word、Outlook、Teams、その他の Microsoft 365 アプリで特定の種類の機密コンテンツを扱う際に、通知が表示される場合があります。これは、クラウド認証情報、日本の個人情報、金融情報、eSolia の機密ラベルが付与されたコンテンツを保護する新しいデータ損失防止ルールの一部です。
>
> 最初の 2 週間は、ルールは通知のみで、何もブロックされません。通知には何が検出されたかと、どう進めればよいかが表示されます。正当なビジネス理由がある場合は、簡単な justification を入力して override できます。
>
> 質問や、理解できない通知があった場合は、[サポート連絡先] までご連絡ください。ブロック開始後よりも、今のうちに混乱を解消したいです。

Phase 3 announcement (English)

> Subject: Reminder: data loss prevention rules begin enforcing on [date]
>
> A reminder that starting [date], the data loss prevention rules you've been seeing notifications about will begin actively blocking the actions they detect, instead of just notifying.
>
> Most users will see no change. The rules block: sharing cloud credentials externally, sharing Japan My Number externally, sharing credit card numbers externally, sharing content marked with Confidential or Restricted labels externally, and a few other narrowly-defined situations.

> If you legitimately need to perform an action the rules block, contact [support contact] for an exception or use the in-product override option where available. Most blocks include an override option with business justification.
>
> Thanks for your patience during the rollout.

Phase 3 announcement (Japanese)

> 件名: リマインド：データ損失防止ルールが [日付] より enforce 開始
>
> リマインドです。[日付] より、これまで通知だけだったデータ損失防止ルールが、検出したアクションを実際にブロックするようになります。
>
> ほとんどのユーザーにとって変化はありません。ルールがブロックするのは：クラウド認証情報の外部共有、Japan My Number の外部共有、クレジットカード番号の外部共有、Confidential または Restricted ラベルが付与されたコンテンツの外部共有、その他いくつかの限定的な状況です。
>
> ルールがブロックするアクションを正当に実行する必要がある場合は、[サポート連絡先] まで例外申請してください。または、利用可能な場合はアプリ内の override オプション（business justification 入力）を使用してください。
>
> 展開期間中のご協力ありがとうございます。

Appendix C: Quick reference sequence

For repeat use or handoff to a colleague:

```
Day 0:    Phase 0 verification (15-20 min)
          Phase 1 deployment of all 8 policies in test mode (60-75 min)
Days 1-3: Daily check of Activity Explorer
Day 7:    Mid-point review, document false positives
Day 14:   Phase 2 transition (30 min) + user announcement
Days 15-28: Field user questions, track overrides
Day 28:   Phase 3 transition (30 min) + user announcement
Day 29:   Verification testing of enforce mode
Day 30+:  Steady state - monthly/quarterly/annual cycles
```

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST