Purview DLP Baseline Policy Reference

Purview DLP ベースラインポリシー リファレンス

April 11, 2026 / 2026 年 4 月 11 日

English Version

See page 20 →

日本語版

3 ページへ →

eSolia

Purview DLP ベースラインポリシー リファレンス

2026 年 4 月 11 日

目次

クライアントテナントに Microsoft Purview Data Loss Prevention を展開する際のリファレンスです。全クライアント共通で適用する eSolia ベースラインと、SMB、コンサルティング、FSA 規制対象の 3 つのオーバーレイバリアントを定義します。デリバリープロジェクトの出発点として使ってください。クライアント提出用の文書ではありません。

このリファレンスを使う場面

新規クライアントテナントで Purview DLP をセットアップするとき、既存クライアントの DLP 態勢をレビューするとき、コンプライアンス案件のスコープを作成して監査に説明できる出発点が必要なときに使います。ベースラインは意図的に保守的に作ってあります。どのルールも監査人に説明できるものであり、かつ合理的なエンドユーザーを驚かせないものに限定しています。クライアント固有のチューニングは、ベースラインの代わりではなくベースラインの上に乗せる形で行います。

提案書や SOW を作るなら、この文書は社内スコープ作成用とし、クライアント向けには別バージョンを書いてください。このファイルをクライアントに送らないこと。

前提条件

以下のポリシーを展開する前に、クライアントテナントで次が揃っている必要があります。

- **ライセンス:** Microsoft 365 E5、Microsoft 365 E5 Compliance アドオン、または Microsoft 365 E5 Information Protection and Governance アドオン。E3 のみのテナントでは基本的な SIT とラベルは展開できますが、trainable classifier、endpoint DLP、auto-labeling が使えません。ライセンス議論の段階でクライアントに伝える価値があります。
- **Endpoint DLP の前提条件:** Devices を対象とするポリシーを展開するには、クライアントの Windows と macOS デバイスを Microsoft Purview device monitoring にオンボード済みにする必要があります。特に macOS については `eSolia-Defender-macOS-DLP-Troubleshooting-Runbook-INTERNAL-20260410-ja.md` を参照。オンボーディング手順と既知の落とし穴をまとめています。
- **Sensitivity label の公開:** ラベルベースの DLP ルールが発火するには、sensitivity label の分類体系が存在し、ユーザーに公開されている必要があります。ベースラインでは 7 層分類を前提にしています（セクション 2 参照）。
- **Pay-as-you-go billing のリンク:** 一部の新しい Purview 機能は、従量課金用の Azure サブスクリプションをリンクする必要があります。高度な分類や EDM を必要とするルールを展開する前に、Purview → Settings → DLP → Billing を確認してください。
- **管理者ロール:** ポリシー作成には Security Administrator または Compliance Administrator が必要です。PIM を使っているテナントでは、作業開始前にロールを activate してください。macOS ランブックの PIM activation ノートを参照。

eSolia ベースライン

業種、規模、規制プロファイルに関係なく、全クライアントテナントにこれらのポリシーを展開します。eSolia が支援する組織の最低限の DLP 態勢です。正しく設定されていればノイズは少なく、いずれも「起きてから説明するのは恥ずかしい」系のインシデントを防ぎます。

1. クラウド認証情報の保護

何を検出するか: API キー、SSH 秘密鍵、データベース接続文字列、クラウドプロバイダの認証情報が、ドキュメント、メール、Teams メッセージ、SharePoint や OneDrive へのアップロードに含まれるのを検出します。

なぜベースラインに入れるか: 存在する DLP ポリシーの中で最も ROI が高いものです。設定に 30 分かかり、実際によくあるミスを捕捉し、見逃したときの帰結はクラウド環境全体の侵害になり得ます。GitHub への誤プッシュや Teams への AWS シークレットの誤ペーストから始まった実際の侵害事例は数多く報告されています。

設定:

- **場所:** Exchange、SharePoint、OneDrive、Teams チャット・チャネルメッセージ、Devices
- **条件:** 以下のビルトイン SIT のいずれかを含むコンテンツ
  - 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
- **アクション:**
  - 外部共有をブロック
  - カスタムメッセージでユーザーに通知：「このコンテンツにはクラウド認証情報または認証シークレット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許可されていません。検出が誤りの場合は IT まで連絡してください。」
  - business justification による override を許可（社内共有の false positive 対策）
  - セキュリティチーム宛にインシデントレポートを生成
- **モード:** Enforce（ブロック）

想定される false positive 率: 非常に低い。SIT は密に定義されており、proximity rule と Luhn 形式のバリデーションが含まれます。主な false positive 源は、サンプル認証情報を含むドキュメンテーションです。ドキュメントサイトを SharePoint から除外するか、ドキュメント内でプレースホルダ値を使うことで解決します。

2. Sensitivity label の enforcement

何を検出するか: sensitivity label が付与されたドキュメントが、保護レベルに反する形で移動するのを検出します。

なぜベースラインに入れるか: sensitivity label は成熟した DLP 展開の背骨であり、enforcement ルールと組み合わせて初めて価値を発揮します。ルールがなければラベルは装飾にすぎません。ラベルを機能させるのが我々の仕事です。

eSolia 7 層ラベル分類体系:

優先度	Label (EN)	Label (JA)	内部名	定義	DLP 動作
0	Public	社外一般	eSolia-Public	一般公開承認済み	制限なし
1	Work Share	業務共有	eSolia-WorkShare	業務上の外部共有に適したコンテンツ	制限なし
2	Commercial Papers	商用書類	eSolia-CommercialPapers	契約書、見積書等の商用ドキュメント	制限なし
3	Protected Internal	社内一般	eSolia-ProtectedInternal	eSolia スタッフおよび明示的に許可されたパートナーのみ	外部メールブロック、許可リスト外のクラウドサービスへのアップロードブロック
4	Client Confidential	顧客機密情報	eSolia-ClientConfidential	クライアント固有の機密データ	外部共有ブロック、USB コピーブロック、印刷を audit
5	Confidential	秘密	eSolia-Confidential	機密ビジネス情報、need-to-know ベース	外部共有ブロック、USB コピーブロック、印刷に justification 必須
6	Restricted	極秘	eSolia-Restricted	MNPI、認証情報、法務成果物	メール、USB、クラウドアップロードを含む全ての外部 egress をブロック。クリップボード監査。ラベル付きセキュリティグループ外への社内共有に justification 必須。

両言語のラベル名を全てのラベルに表示してください。バイリンガルのスタッフがどちらの言語で作業していてもラベルを付けられるようにするためです。

設定上の注意:

- ラベルは手動（ユーザー駆動）と auto-labeling の両方で適用する。実際のカバレッジは auto-labeling から出ます。

- 各層の auto-labeling 条件はクライアントごとに文書化すべきです。条件がクライアント固有のコンテンツに依存するからです。よくあるパターン：Legal の SharePoint サイトにあるものは全て自動で Confidential、Japan My Number を含むか client list fingerprint に一致するものは全て自動で Restricted。
- Confidential と Restricted の層では、DLP ルールとは独立に、ラベル自体が暗号化とアクセス制限も enforce するべきです。これはラベル定義内の設定であり、DLP ルールではありません。

モード: Confidential と Restricted は Enforce、Protected Internal は展開後 30 日間 Audit で運用してから enforce に切り替え。

3. 日本の個人情報保護

何を検出するか: Japan My Number（個人番号）、住民票コード、または大量の日本形式の個人データを含むドキュメントやメールの移動を検出します。

なぜベースラインに入れるか: 日本の個人情報保護法（APPI）は、My Number を最高感度の識別子カテゴリとして扱います。権限外の開示は個人情報保護委員会への報告義務を発動し、刑事罰の対象にもなり得ます。eSolia が管理するテナントには全てこのルールを入れます。クライアントが My Number を扱っていないと思っていても入れます。「うちには無いはず」はインシデントの始まり方だからです。

設定:

- **場所:** Exchange、SharePoint、OneDrive、Teams、Devices
- **条件:** 以下のいずれかを含むコンテンツ
  - Japan My Number (Individual Number) — ビルトイン SIT
  - Japan Resident Registration Number — ビルトイン SIT
  - Japan Passport Number — ビルトイン SIT
  - Japan Driver's License Number — ビルトイン SIT
- **マッチ閾値:** 1 件以上（10 件以上ではない。My Number は 1 件でも通知に値する感度）
- **アクション:**
  - 外部共有をブロック
  - USB リムーバブルメディアへのコピーをブロック
  - 英語と日本語の両方でカスタムメッセージをユーザーに通知
  - コンプライアンスチーム宛にインシデントレポートを生成
  - Activity Explorer に高重大度でログ記録
- **モード:** Enforce（ブロック）

想定される false positive: 低いが、ゼロではありません。Japan My Number SIT は 12 桁チェックを使いますが、特定の文脈で任意の 12 桁数字文字列にマッチすることがあります。クライアントが 12 桁の正当な識別子（従業員 ID、プロジェクトコードなど）を持っている場合は、proximity rule を使ったカスタム SIT を作成するか、その ID フォーマットを例外として追加してください。

4. 金融データの保護

何を検出するか: クレジットカード番号（Luhn バリデーション済み）、銀行口座番号、SWIFT コード、その他の決済手段を含むドキュメントや通信を検出します。

なぜベースラインに入れるか: どの組織も何らかの金融データを扱います。金融機関でなくても、請求書、経費精算、ベンダー支払情報があります。日本でのクレジットカード番号漏洩のコストは米国 PCI-DSS の施行ほど劇的ではありませんが、それでも報告対象であり、損害もあります。

設定:

- **場所:** Exchange、SharePoint、OneDrive、Teams、Devices
- **条件:** 以下のいずれかを含むコンテンツ
  - Credit Card Number（Luhn バリデーション付きのビルトイン SIT）
  - Japan Bank Account Number
  - International Bank Account Number (IBAN)
  - SWIFT Code
  - US/UK Bank Account Number（海外接点のあるクライアント向け）
- **マッチ閾値:** クレジットカードは 1 件以上、銀行口座は 1 件以上
- **アクション:**
  - メールまたはクラウドアップロードによる外部共有をブロック
  - Finance セキュリティグループ外への社内共有に justification 必須
  - USB コピーを audit
- **モード:** Enforce

5. ベースライン外部共有制御

何を検出するか: コンテンツ分類に関係なく、sensitive な SharePoint サイトや OneDrive フォルダからの外部共有を検出します。

なぜベースラインに入れるか: コンテンツベースの DLP は強力ですが万能ではありません。「Legal サイトから外部へは何も出さない」というポリシーは、コンテンツ分類が失敗した場合やラベルが付与されなかった場合をカバーする belt-and-suspenders レイヤーとして機能します。

設定:

- **場所:** SharePoint（特定サイト）、OneDrive
- **条件:** 組織外のユーザーとのコンテンツ共有
- **アクション:**
  - 「Restricted」とタグ付けされたサイト（Legal、HR、Finance、クライアント固有のプロジェクトサイト）：外部共有を完全にブロック
  - それ以外のサイト：ユーザーに通知し justification を要求
- **モード:** Restricted サイトは Enforce、一般サイトは Audit

このルールはクライアントごとのセットアップが必要です。どの SharePoint サイトが Restricted かを特定する作業をオンボーディングプロジェクトでクライアントと一緒に行ってください。

オーバーレイ A: SMB バリアント

業種固有の規制義務がない中小規模のクライアント向け。ベースラインに以下を追加します。

A.1 退職予定者の保護

何を検出するか: 退職予定者としてフラグが立っている従業員による異常なファイルアクセスパターンを検出します。

なぜここに入れるか: SMB で最も一般的なデータ持ち出しのシナリオは、退職予定の従業員がクライアントリスト、案件パイプライン、設計ファイルなどを退職時にコピーすることです。悪意ある内部者というより、正直な勘違いであることが多い。人は「自分の仕事」を持っていって良いと思っているからです。

設定:

- 実装は伝統的な DLP ではなく Microsoft Purview Insider Risk Management を使いますが、同じコンテンツ分類インフラを共有します。
- Entra ID に「Departing Employees」というセキュリティグループを作成し、退職通知があったら HR が追加する運用にします。
- Insider Risk Management → Policies → ポリシー作成 → 「Data leaks by priority users」
- 監視対象アクティビティ：大量ファイルダウンロード、USB コピー、外部メール転送、SharePoint 一括アクセス
- 監視期間：グループ追加日から、最終勤務日後 30 日間まで
- アラート閾値：Medium（false positive 率に応じて調整）
- アラート通知先：HR と IT セキュリティ

重要: これには、退職通知があった時点で従業員を Departing Employees グループに追加する文書化された HR プロセスが必要です。プロセスなしの DLP ツールはただのノイズです。

A.2 軽量なクライアントデータ保護

何を検出するか: クライアント識別子を含むドキュメントやメールを、クライアント辞書と照合して検出します。

なぜここに入れるか: SMB は通常、管理可能なクライアントリスト（数十から低三桁）を持っており、keyword dictionary アプローチが実用的です。このルールは、誤って別クライアント宛のメールに間違ったクライアントのデータを添付するケースを捕捉します。

設定:

- Keyword dictionary を作成：Purview → Data Classification → Classifiers → Keyword dictionaries → Create → 「Client Names and Domains」
- 投入内容：クライアント企業名、クライアント主要ドメイン、よく使われる子会社・製品名。CRM エクスポートから四半期ごとにメンテナンス。
- カスタム SIT を作成し、上記の dictionary を match threshold 5 件以上で参照（複数のクライアントに言及するドキュメントを捕捉。これは「クライアントリストを含む」の妥当な代理指標）
- ポリシーアクション：ユーザー通知付きで Audit。ブロックしない。false positive が多すぎるため。
- モード：Audit only

このルールは enforce ではなく、意図的に informational として運用します。目的は月次コンプライアンスレビュー用のアクティビティを生成することであり、業務を妨げることではありません。

A.3 標準デバイス制御

何を検出するか: 未承認の USB 使用、sensitive なコンテンツの印刷を検出します。

なぜここに入れるか: SMB は heavy-handed なエンドポイント制限を嫌うことが多いですが、最小限のデバイス制御レイヤーで最悪のケースは防げます。

設定:

- Endpoint DLP → Device control
- Confidential と Restricted ラベルのコンテンツを USB リムーバブルメディアにコピーすることを **ブロック**
- コンテンツに関係なく全ての USB コピーを **Audit**（forensic trail として有用）
- ラベル付きコンテンツの印刷を **Audit**
- その他のデバイスアクションは **許可**。USB を全面的にロックダウンするのではなく、ラベル付きコンテンツを保護するのが目的。

オーバーレイ B: コンサルティングバリアント

コンサルティング、法務、プロフェッショナルサービス、その他の案件主体のクライアント向け。主要な sensitive asset がクライアント成果物、案件デリバラブル、マルチクライアント分離であるケース。ベースラインに以下を追加します。

B.1 複数クライアントドメインの検出

何を検出するか: 複数のクライアント識別子を同時に含むドキュメントを検出します。クロスクライアント汚染やデータ混在の古典的なシグナルです。

なぜここに入れるか: コンサルティングファームには厳格なクライアント分離義務があります。クライアント B へのデリバラブルに誤ってクライアント A のデータが含まれると、機密漏洩と責任問題の両方になります。このルールはテナントを出る前にそれを捕捉します。

設定:

- Keyword dictionary を作成：「Client Names and Domains (Consulting)」
- CRM/案件管理システムから投入：全アクティブクライアントの法人名、主要ドメイン、主要子会社名
- カスタム SIT :「Multiple Client Identifiers」、dictionary からの match threshold 10 件以上を単一ドキュメント内で要求
- ポリシー場所：SharePoint、OneDrive、Exchange、Devices
- アクション：外部共有をブロック、社内共有に justification 必須、案件マネージャーにアラート
- モード：外部は Enforce、社内は Audit

10 件以上という閾値は意図的に高めにしてあります。クライアントリストや複合デリバラブルを捕捉したいのであって、競合への言及や業界への参照を正当に含むケースは捕捉しません。

B.2 案件コードのフィンガープリント

何を検出するか: 標準化された案件テンプレート（SOW、デリバラブルテンプレート、請求書テンプレート）から派生したドキュメントが、案件チーム外で共有されるのを検出します。

なぜここに入れるか: コンサルティングファームは案件をまたいで文書テンプレートを再利用します。フィンガープリントにより、テンプレートとして始まった文書を追跡し、別のクライアントの手に渡らないようにできます。

設定:

- Purview → Data Classification → Classifiers → Document fingerprints → Create
- 主要テンプレートのブランク版をアップロード :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、案件契約書テンプレート
- DLP ルールを作成し、条件に「Content matches document fingerprint」で上記テンプレートのいずれかを指定
- アクション：ドキュメントに sensitivity label（Confidential 以上）の付与を要求。付与されていない場合は共有前のラベル付与を要求。
- モード：Enforce

B.3 Trainable classifier: ソースコード

何を検出するか: ドキュメントやメールに含まれるソースコードを検出します。

なぜここに入れるか: 多くのコンサルティング案件にコードデリバラブルが含まれますが、コードはソース管理を通すべきであり、メール添付で移動すべきではありません。このルールは誤った経路によるコードの共有を捕捉します。

設定:

- ビルトインの「Source Code」trainable classifier を使用
- 場所：Exchange、Teams、Devices（endpoint）
- アクション：ユーザーに通知し、クライアントの Git リポジトリの使用を提案、justification で override 可能
- モード：初期は Audit、30 日後に Warn へアップグレード

B.4 Information barriers（競合クライアント案件を持つコンサルティングファーム向け）

何を検出するか: 競合するクライアントに取り組むチーム間の通信またはファイルアクセスを検出します。

なぜここに入れるか: コンサルティングファームが競合する 2 つのクライアントと同時に案件を持っている場合、案件チーム間の情報漏洩を防ぐための正式な information barrier が必要になることがあります。組織的な問題であり、技術だけの問題ではありません。

設定: Purview → Information barriers → 各競合案件チーム用のセグメントを作成し、それらの間の barrier ポリシーを定義します。Microsoft の Information Barriers ドキュメントを参照してください。設定は runbook のセクションで扱うには固有すぎます。

重要: Information barriers は慎重な計画と法務レビューが必要です。独断で実装しないこと。

オーバーレイ C: FSA 規制対象バリアント

金融庁の監督下にある金融サービスクライアント向け：ファンド運用会社、投資アドバイザー、信託銀行、証券会社など。このオーバーレイは、ベースラインに加えて、金融庁サイバーセキュリティ監督ガイドラインと J-SOX コンプライアンスで要求される重要な追加制御を前提とします。

C.1 重要な未公開情報（MNPI）の保護

何を検出するか: MNPI を含むドキュメント（ディールメモ、発表前の決算レポート、投資テーゼ、取引戦略、未公表の会社アクションなど）を検出します。

なぜここに入れるか: 金融庁のサイバーセキュリティガイドラインは、非公開情報の権限外開示を防ぐ制御を明示的に求めています。MNPI の権限外開示はインサイダー取引調査、規制アクション、刑事責任を発動し得ます。

設定:

- 分類体系に「MNPI」sensitivity label を作成（Restricted のサブラベル）
- 標準化された MNPI ドキュメントタイプの document fingerprint を作成：ディールメモテンプレート、決算レポートテンプレート、投資委員会議事録テンプレート
- Auto-labeling ポリシー：上記 fingerprint のいずれかに一致するコンテンツ、または MNPI SharePoint サイト内のコンテンツ、または特定の MNPI キーワード（「発表前」「非公開」など）を含むコンテンツに MNPI ラベルを適用
- DLP ルール：MNPI ラベル付きコンテンツはいかなる状況でも外部共有不可、USB コピー不可、事前承認なしの印刷不可、MNPI 承認済みセキュリティグループ外のユーザーとの共有不可
- 監査証跡：MNPI ラベル付きコンテンツへの全アクセスを Advanced Audit で 10 年保持
- モード：Enforce（ブロック）、ユーザー override 不可

C.2 リサーチとトレーディングの間の information barrier

何を検出するか: リサーチチームとトレーディングチームの間の通信、ドキュメント共有、会議出席を検出します。

なぜここに入れるか: リサーチとトレーディングの間の「Chinese wall」は、リサーチを生成し取引も執行するファームにとって基本的な要件です。従来の物理的分離だけでは不十分であり、barrier は Teams、SharePoint、メールにも存在する必要があります。

設定:

- Entra ID セキュリティグループ：「Research Team」と「Trading Team」
- Purview → Information barriers → Segments → 各グループ用のセグメントを作成
- ポリシー：Research ↔ Trading を双方向でブロック
- 対象アクション：Teams メッセージング（1 on 1 とチャネル）、カレンダー会議招待、SharePoint サイトメンバーシップ、OneDrive ダイレクト共有、メール
- 例外：コンプライアンスチームは両セグメントを可視化できる

重要: Information barriers は片道ドアです。一度展開すると解除が disruptive になります。クライアントの法務・コンプライアンス機能と事前に協議し、ロールアウトを慎重に段階化してください。

C.3 投資家データの保護

何を検出するか: 投資家の個人情報、ファンドポジション、投資家向け通信を含むドキュメントの移動を検出します。

なぜここに入れるか: 金融庁のファンド運用監督は、投資家データを特別に保護された対象として扱います。ファンドマネージャーのクライアントは、投資家の身元、保有、通信の権限外開示を防ぐ制御を実証する必要があります。

設定:

- 「Investor Confidential」sensitivity label を作成（Restricted のサブラベル）
- Investor Relations SharePoint サイトと特定の投資家通信フォルダ内のコンテンツに自動ラベル付け
- 投資家の法人名と主要連絡先ドメインの keyword dictionary を作成（ファンド運用システムからメンテナンス）
- カスタム SIT：「Multiple Investor Identifiers」、dictionary から 3 件以上の投資家名にマッチ（クライアントバリアントより低い閾値。複数投資家を含むドキュメントは既に懸念対象だから）
- DLP ルール：外部共有ブロック、非承認先へのコピーブロック、IR チーム外への社内共有全てに justification 必須、全アクセスを高重大度でログ記録して audit
- モード：Enforce

C.4 Advanced Audit の保持

何を検出するか: これ自体は DLP ルールではなく、他の全てのルールの forensic 価値を支える設定です。

なぜここに入れるか: 金融庁検査は数年遡ることがあります。Purview の標準監査保持は 180 日であり、規制対応には不十分です。FSA 規制対象クライアントは、全 DLP 関連イベントについて Advanced Audit を有効にし、10 年保持を設定すべきです。

設定:

- Purview → Settings → Audit → Advanced Audit が有効であることを確認（E5 ライセンス必須）
- Purview → Audit → Retention policies → Create → DLP イベントとファイルアクセスイベントを 10 年保持
- 保持ポリシーをクライアントのコンプライアンスドキュメントに記録
- コールドストレージへの監査ログエクスポートを四半期ごとの運用タスクとして含める

C.5 投資討議のコミュニケーションコンプライアンス

何を検出するか: 投資判断、推奨、クライアントポジションについての Teams メッセージ、メール、会議トランスクリプトがコンプライアンスポリシーに違反する形で行われるのを検出します。

なぜここに入れるか: 金融庁の規則は投資推奨に関する通信の監督を要求します。これは DLP ではなく Communication Compliance のユースケースですが、コンテンツ分類のインフラは両方で共有されます。

設定:

- Purview → Communication Compliance → Policies → Create
- テンプレート：日本語と英語の投資用語のカスタム classifier を持つ sensitive info types
- 監視スコープ：トレーディングチーム、リサーチチーム、クライアント対応のアドバイザー
- レビューキュー：コンプライアンスチーム
- モード：初期はサンプリング付き Audit（マッチの 5% をレビュー）、発見事項に基づいてスケール

展開アプローチ

どのオーバーレイを展開する場合でも、以下のシーケンスに従ってください。一気に DLP を展開すると目に見える disruption が発生し、プロジェクトの信頼性が損なわれ、チューニングも不可能になります。

フェーズ 1: Audit mode（1〜2 週目）

全てのルールをユーザー通知なしの audit mode で展開します。Activity Explorer でマッチを観察します。目的は、エンドユーザーに何か目に見えることが起きる前に、クライアントの実環境でルールが何を捕捉するかを理解することです。

想定される結果：false positive の発見、ルールが干渉する正当なビジネスプロセスの発見、コンテンツ分類のギャップ（マッチすべきなのにしないコンテンツ）の発見。全て正常な発見事項であり、フェーズ 2 の前に対処します。

フェーズ 2: Notify mode（3〜4 週目）

ルールマッチ時のユーザー通知をオンにします。ブロックはまだしません。ユーザーが「このアクションは DLP ルールをトリガーしました」というメッセージを見始めます。目的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です。

想定される結果：ユーザーからの質問の波（「同僚にメールしただけなのになぜ通知が来るのか」）、いくつかの正当な例外要求、DLP の存在に対する認知度の全般的上昇。質問に素早く対応すること。展開の雰囲気を決める段階です。

フェーズ 3: Enforce（5 週目以降）

ブロックが設定されているルールのブロックを有効化します。情報収集用のルールは audit-only のまま。

想定される結果 :少数のブロックされたアクション、初期フェーズでは捕捉されなかった真のビジネスニーズに関するユーザーからのエスカレーション、定常運用の開始。

フェーズ 4: 定常状態（継続）

月次で Activity Explorer をレビュー、四半期ごとにクライアントとポリシー効果をレビュー、年次でクライアントのビジネス変化と Microsoft の機能更新に対してベースライン全体をレビュー。

チューニングと例外処理

どのベースライン展開もクライアント固有のチューニングが必要になります。よくある調整事項：

- **クライアント自身のドキュメント SharePoint サイトを認証情報検出ルールから除外**（ドキュメント内にサンプル認証情報がある）
- **クライアントの承認済みクラウドサービスの許可リストエントリを追加**して、upload-to-cloud ルールが自社ファイル共有への正当なアップロードで発火しないようにする
- **sensitive content への正当なアクセスを持つユーザーの例外グループを追加**（金融データルールに対しては Finance チーム、契約テンプレートに対しては Legal チーム）
- **keyword dictionary SIT のマッチ閾値を調整**、観察された false positive 率に基づいて
- **クライアント固有の sensitive info type を作成**、固有の識別子（社内プロジェクトコード、製品名、従業員 ID フォーマット）向け

全てのチューニングはクライアントの DLP 実装ログに文書化し、テナントドキュメントと一緒に保持してください。将来の eSolia スタッフが特定の例外がなぜ存在するかを理解できるようにするためです。

ベースラインに意図的に入れていないもの

Purview 展開ではよく見られるが、eSolia ベースラインには意図的に含めていないポリシーがいくつかあります。なぜかを知っておくのは、クライアントから質問されたときに答えるために大事です。

キーワードマッチによる全メールコンテンツスキャン。false positive 率が高く、価値は低く、ユーザーにとって煩わしい。具体的な要求と正当化があるときだけ展開する。

添付ファイル付き外部メールの全面ブロック。維持できないほどの friction を作ります。ユーザーは個人メールで回避するため、元のリスクより悪化します。

全ドキュメントの透かし。sensitivity label を通じて利用可能ですが、実用性は低く、見た目も悪いことが多い。具体的な要件があるときだけ展開する。

「company confidential」スタイルコンテンツ用の trainable classifier。汎用ビジネス機密コンテンツ用のビルトイン trainable classifier は信頼できません。代わりに sensitivity label と明示的な SIT を使ってください。

個人クラウドストレージへの全アクセスブロック。 DLP レイヤーより、ネットワークレイヤー（Cloudflare Zero Trust、ファイアウォール DNS フィルタリング）で処理する方が適切です。この目的の DLP ポリシーはワークフロー内で発火するタイミングが遅すぎます。

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 Baseline Policy Reference

April 11, 2026

Contents

> eSolia INTERNAL — Not for distribution outside eSolia

A reference for deploying Microsoft Purview Data Loss Prevention policies in client tenants. Describes the eSolia baseline that applies to every client, plus three overlay variants for SMB, consulting, and FSA-regulated clients. Use this as a starting point in delivery projects — it is not a client-facing document.

When to use this reference

Reach for this document when you're setting up Purview DLP in a new client tenant, when you're reviewing an existing client's DLP posture, or when you're scoping a compliance engagement and need a defensible starting point. The baseline is deliberately conservative — every rule in it should be justifiable to an auditor, and none of it should surprise a reasonable end user. Client-specific tuning happens on top of the baseline, not in place of it.

If you're building a proposal or statement of work, use this document for your internal scoping and write a client-friendly version for the deliverable. Do not send this file to clients.

Prerequisites

Before you deploy any of these policies, the client tenant needs:

- **Licensing:** Microsoft 365 E5, Microsoft 365 E5 Compliance add-on, or Microsoft 365 E5 Information Protection and Governance add-on. E3-only tenants can deploy a subset (basic SITs and labels) but lose trainable classifiers, endpoint DLP, and auto-labeling — worth flagging in the client's licensing discussion before you start.
- **Endpoint DLP prerequisites:** For any policy targeting Devices, the client's Windows and macOS devices must be onboarded to Microsoft Purview device monitoring. For macOS specifically, see `eSolia-Defender-macOS-DLP-Troubleshooting-Runbook-INTERNAL-20260410-en.md` for onboarding and known pitfalls.
- **Sensitivity labels published:** A sensitivity label taxonomy must exist and be published to users before label-based DLP rules can fire. The baseline assumes a 4-tier taxonomy (see Section 2).
- **Pay-as-you-go billing link:** Some newer Purview features require an Azure subscription linked for consumption billing. Check Purview → Settings → DLP → Billing before deploying rules that need advanced classification or EDM.
- **Admin roles:** Security Administrator or Compliance Administrator for policy creation. In tenants using PIM, activate before starting — see the PIM activation note in the macOS runbook.

The eSolia Baseline

Every client tenant gets these policies regardless of industry, size, or regulatory profile. They represent the minimum acceptable DLP posture for any organization eSolia supports. None of them should generate significant noise when correctly configured, and all of them prevent incidents that would be embarrassing to explain in hindsight.

1. Cloud credential protection

What it catches: Accidental sharing of API keys, SSH private keys, database connection strings, and cloud provider credentials in documents, emails, Teams messages, or files uploaded to SharePoint and OneDrive.

Why it's in the baseline: This is the highest ROI DLP policy in existence. It takes 30 minutes to configure, catches a genuine and common mistake, and the consequence of missing it can be a complete cloud environment compromise. The number of real-world breaches that started with a GitHub push or a Teams paste of an AWS secret is substantial.

Configuration:

- **Locations:** Exchange, SharePoint, OneDrive, Teams chat and channel messages, Devices
- **Conditions:** Content contains any of the following built-in sensitive info types:
  - 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
- **Actions:**
  - Block external sharing
  - Notify user with a custom message: "This content appears to contain cloud credentials or authentication secrets. Sharing credentials externally is not permitted. If this detection is incorrect, please contact IT."
  - Allow override with business justification (for internal sharing false positives)
  - Generate incident report to security team
- **Mode:** Enforce (block)

Expected false positive rate: Very low. The SITs are tightly defined and include proximity rules and Luhn-style validation. Primary source of false positives is documentation that shows example credentials — solved by excluding your documentation SharePoint site or using placeholder values in docs.

2. Sensitivity label enforcement

What it catches: Movement of documents marked with sensitivity labels in ways that violate the intended protection level.

Why it's in the baseline: Sensitivity labels are the backbone of every mature DLP deployment, and their value is only realized when paired with enforcement rules. Without rules, labels are decorative. Our job is to make them functional.

The eSolia 7-tier label taxonomy:

Priority	Label (EN)	Label (JA)	Definition	DLP behavior
0	Public	社外一般	Approved for public consumption	No restrictions
1	Work Share	業務共有	Routine external sharing with specific contacts	No restrictions (content is meant for external sharing)
2	Commercial Papers	商用書類	Client-facing business documents requiring processing	No restrictions (content is shared with specific client contacts)
3	Protected Internal	社内一般	Internal-only, baseline protection	Block external email, block upload to non-allowlisted cloud services
4	Client Confidential	顧客機密情報	Client data under duty of care	Block external sharing, block USB copy, audit print
5	Confidential	秘密	Sensitive internal (HR, contracts, legal)	Block external sharing, block USB copy, require justification for print
6	Restricted	極秘	Highest classification (financials, strategy, MNPI)	Block all external egress including email, USB, and cloud upload. Audit clipboard. Require justification for internal sharing outside the labeled security group.

Both the EN and JA label names should appear on every label so bilingual staff can apply them in whichever language they're working in. See the Purview Sensitivity Label Taxonomy and Application Guide for the full reference including user-facing descriptions and decision guidance.

Configuration notes:

- Apply labels through both manual (user-driven) and auto-labeling policies. Auto-labeling is where the real coverage comes from.
- Auto-labeling conditions for each tier should be documented per client, because the conditions depend on client-specific content. A common pattern: auto-apply Confidential to anything in the Legal SharePoint site; auto-apply Restricted to anything containing Japan My Number or matching the client list fingerprint.
- Labels should also enforce encryption and access restrictions on Confidential and Restricted tiers, independently of DLP. This is a setting within the label definition, not the DLP rule.

Mode: Enforce for Confidential and Restricted, Audit for Protected Internal for the first 30 days of deployment then enforce.

3. Japanese personal data protection

What it catches: Movement of documents or emails containing Japan My Number (個人番号), Japan resident registration numbers, or large quantities of Japan-format personal data.

Why it's in the baseline: Japan's Personal Information Protection Act (APPI) treats My Number as the highest-sensitivity identifier category. Unauthorized disclosure triggers mandatory reporting to the Personal Information Protection Commission and can result in criminal penalties. This rule exists in every eSolia-managed tenant regardless of whether the client thinks they handle My Number data, because "we don't think we have any" is how incidents happen.

Configuration:

- **Locations:** Exchange, SharePoint, OneDrive, Teams, Devices
- **Conditions:** Content contains any of:
  - Japan My Number (Individual Number) — built-in SIT
  - Japan Resident Registration Number — built-in SIT
  - Japan Passport Number — built-in SIT
  - Japan Driver's License Number — built-in SIT
- **Match threshold:** 1 or more (not 10+ — a single My Number is sensitive enough to warrant the notification)
- **Actions:**
  - Block external sharing
  - Block copy to USB removable media
  - Notify user with custom message in both English and Japanese
  - Generate incident report to compliance team
  - Log to Activity Explorer with high severity
- **Mode:** Enforce (block)

Expected false positives: Low, but not zero. The Japan My Number SIT uses a 12-digit check but can match random 12-digit numeric strings in certain contexts. If the client has legitimate 12-digit identifiers

(employee IDs, project codes, etc.) that collide, create a custom SIT with proximity rules or add the specific ID format as an exception.

4. Financial data protection

What it catches: Credit card numbers (Luhn-validated), bank account numbers, SWIFT codes, and similar payment instruments in documents or communications.

Why it's in the baseline: Every organization handles some financial data even if they're not a financial institution — invoices, expense reports, vendor payment information. The cost of a credit card number leak in Japan is not as dramatic as under PCI-DSS US enforcement, but it's still reportable and still damaging.

Configuration:

- **Locations:** Exchange, SharePoint, OneDrive, Teams, Devices
- **Conditions:** Content contains any of:
  - Credit Card Number (built-in SIT with Luhn validation)
  - Japan Bank Account Number
  - International Bank Account Number (IBAN)
  - SWIFT Code
  - US/UK Bank Account Number (for clients with international exposure)
- **Match threshold:** 1+ for credit cards, 1+ for bank accounts
- **Actions:**
  - Block external sharing via email or cloud upload
  - Require justification for internal sharing outside Finance security group
  - Audit USB copy
- **Mode:** Enforce

5. Baseline external sharing controls

What it catches: External sharing of any content from sensitive SharePoint sites or OneDrive folders, regardless of content classification.

Why it's in the baseline: Content-based DLP is powerful but not infallible. A policy that says "nothing leaves the Legal site to external recipients" is a useful belt-and-suspenders layer that catches cases where content classification failed or labels weren't applied.

Configuration:

- **Locations:** SharePoint (specific sites), OneDrive
- **Conditions:** Content is shared with people outside the organization
- **Actions:**
  - For sites tagged "Restricted" (Legal, HR, Finance, client-specific project sites): Block external sharing entirely
  - For all other sites: Notify user and require justification
- **Mode:** Enforce for Restricted sites, Audit for general sites

This rule requires some per-client setup — identifying which SharePoint sites are Restricted. Work with the client to list them during the onboarding project.

Overlay A: SMB Variant

For small and mid-sized clients without industry-specific regulatory obligations. The baseline plus these additions.

A.1 Departing employee protection

What it catches: Unusual file access patterns from employees flagged as leaving the organization.

Why it's here: The most common data exfiltration scenario in SMBs is a departing employee copying client lists, deal pipelines, or design files on their way out. This is less about malicious insiders and more about honest misunderstandings — people think they're allowed to take "their work" with them.

Configuration:

- Implemented via Microsoft Purview Insider Risk Management, not traditional DLP, but uses the same content classification infrastructure.
- Create a security group in Entra ID called "Departing Employees" that HR populates when notice is given.
- In Insider Risk Management → Policies → Create policy → "Data leaks by priority users"
- Monitored activities: bulk file downloads, USB copies, external email forwarding, SharePoint bulk access
- Monitoring window: From date added to the group, for 30 days after their last day
- Alert threshold: Medium (tune based on false positive rate)
- Alert notifications: HR and IT security

Important: This requires a documented HR process for adding employees to the Departing Employees group when notice is given. DLP tooling without process is just noise.

A.2 Light-touch client data protection

What it catches: Documents and emails containing client identifiers when the client name matches a client dictionary.

Why it's here: SMBs typically have a manageable client list (dozens to low hundreds), which makes a keyword dictionary approach practical. This catches cases where someone accidentally attaches the wrong client's data to an email to a different client.

Configuration:

- Create a keyword dictionary: Purview → Data Classification → Classifiers → Keyword dictionaries → Create → "Client Names and Domains"
- Populate with: client company names, client primary domains, and common subsidiary/product names. Maintain quarterly from CRM export.
- Create a custom SIT referencing the dictionary with a match threshold of 5+ (catches documents mentioning multiple clients, which is a reasonable proxy for "contains a client list")
- Policy action: Audit with user notification. Do not block — too many false positives.
- Mode: Audit only

This rule is deliberately informational rather than enforcing. Its purpose is to generate activity for monthly compliance reviews, not to prevent work.

A.3 Standard device controls

What it catches: Unauthorized USB usage, print of sensitive content.

Why it's here: SMBs often don't want heavy-handed endpoint restrictions, but a minimal device control layer prevents the worst cases.

Configuration:

- Endpoint DLP → Device control
- **Block** copy of Confidential and Highly Confidential labeled content to USB removable media
- **Audit** all USB copies regardless of content (useful forensic trail)
- **Audit** print of labeled content
- **Allow** other device actions — this isn't about locking down USB entirely, it's about protecting labeled content.

Overlay B: Consulting Variant

For clients in consulting, legal, professional services, and similar engagements where the primary sensitive asset is client work product, engagement deliverables, and multi-client separation. The baseline plus these additions.

B.1 Multi-client domain detection

What it catches: Documents containing identifiers from multiple clients simultaneously — a classic signal of cross-client contamination or data mixing.

Why it's here: Consulting firms have strict client separation obligations. A deliverable that accidentally includes data from Client A in a document for Client B is both a confidentiality breach and a liability issue. This rule catches that before it leaves the tenant.

Configuration:

- Create keyword dictionary: "Client Names and Domains (Consulting)"
- Populate from CRM/engagement management system: all active client legal names, primary domains, and major subsidiary names
- Custom SIT: "Multiple Client Identifiers" with match threshold 10+ from the dictionary within a single document
- Policy locations: SharePoint, OneDrive, Exchange, Devices
- Action: Block external sharing, require justification for internal sharing, alert to engagement manager
- Mode: Enforce for external, audit for internal

The 10+ threshold is deliberately high — you want to catch client lists and combined deliverables, not legitimate mentions of competitors or industry references.

B.2 Engagement code fingerprinting

What it catches: Documents derived from standardized engagement templates — statements of work, deliverable templates, invoice templates — being shared outside the engagement team.

Why it's here: Consulting firms reuse document templates across engagements. Fingerprinting lets you track documents that started life as a template and ensure they don't end up in the wrong client's hands.

Configuration:

- Purview → Data Classification → Classifiers → Document fingerprints → Create
- Upload blank versions of key templates: SOW template, deliverable template, invoice template, engagement letter template
- Create DLP rule with condition: "Content matches document fingerprint" for any of the templates
- Action: Require the document to also have a sensitivity label (Confidential or higher) — if it doesn't, require labeling before allowing sharing
- Mode: Enforce

B.3 Trainable classifier: source code

What it catches: Source code in documents or emails.

Why it's here: Many consulting engagements involve code deliverables, and code should travel through source control, not email attachments. This rule catches accidental code sharing via the wrong channel.

Configuration:

- Use the built-in “Source Code” trainable classifier
- Location: Exchange, Teams, Devices (endpoint)
- Action: Notify user, suggest using the client’s Git repository, allow override with justification
- Mode: Audit initially, upgrade to Warn after 30 days

B.4 Information barriers (for consulting firms with competing-client engagements)

What it catches: Communications or file access between teams working on competing clients.

Why it’s here: If the consulting firm has engagements with two competing clients simultaneously, they may need formal information barriers to prevent information leakage between engagement teams. This is organizational, not just technical.

Configuration: Purview → Information barriers → create segments for each competing engagement team, define barrier policies between them. See Microsoft’s Information Barriers documentation for details — the configuration is specific enough that a runbook section can’t do it justice.

Important: Information barriers require careful planning and legal review. Do not implement unilaterally.

Overlay C: FSA-Regulated Variant

For financial services clients subject to Financial Services Agency supervision: fund management firms, investment advisors, trust banks, securities firms, and similar. This overlay assumes the baseline plus significant additional controls required by FSA cybersecurity supervision guidelines and J-SOX compliance.

C.1 Material non-public information (MNPI) protection

What it catches: Documents containing MNPI — deal memoranda, earnings reports pre-release, investment theses, trading strategies, pre-announcement corporate actions.

Why it's here: FSA cybersecurity guidelines explicitly call for controls preventing unauthorized disclosure of non-public information. Unauthorized MNPI disclosure can trigger insider trading investigations, regulatory action, and criminal liability.

Configuration:

- Create a "MNPI" sensitivity label in the taxonomy (sub-label under Highly Confidential)
- Create document fingerprints for standardized MNPI document types: deal memo template, earnings report template, investment committee minutes template
- Auto-labeling policy: Apply MNPI label to content matching any of the fingerprints, OR content in the MNPI SharePoint site, OR content containing specific MNPI keywords ("pre-announcement", "non-public", etc.)
- DLP rule: Content labeled MNPI cannot be shared externally under any circumstances, cannot be copied to USB, cannot be printed without pre-authorization, cannot be shared with users outside the MNPI-authorized security group
- Audit trail: All access to MNPI-labeled content logged to Advanced Audit with 10-year retention
- Mode: Enforce (block) with no user override permitted

C.2 Information barriers between research and trading

What it catches: Communications, document sharing, or meeting attendance between the research team and the trading team.

Why it's here: The "Chinese wall" between research and trading is a fundamental requirement for firms that both produce research and execute trades. Traditional physical separation is no longer sufficient — the barrier must exist in Teams, SharePoint, and email as well.

Configuration:

- Entra ID security groups: "Research Team" and "Trading Team"
- Purview → Information barriers → Segments → Create segment for each
- Policies: Research ↔ Trading is blocked bidirectionally
- Covered actions: Teams messaging (1-on-1 and channels), calendar meeting invites, SharePoint site membership, OneDrive direct sharing, email
- Exceptions: Compliance team has visibility into both segments

Important: Information barriers are a one-way door. Once deployed, they're disruptive to undo. Work with the client's legal and compliance functions before deploying, and stage the rollout carefully.

C.3 Investor data protection

What it catches: Movement of documents containing investor personal information, fund positions, or investor communications.

Why it's here: FSA fund management supervision treats investor data as specially protected. Client fund managers must demonstrate controls preventing unauthorized disclosure of investor identities, holdings, and communications.

Configuration:

- Create a sensitivity label "Investor Confidential" (sub-label under Highly Confidential)
- Auto-label content in the Investor Relations SharePoint site and specific investor communication folders
- Create a keyword dictionary of investor legal names and primary contact domains (maintained from the fund management system)
- Custom SIT: "Multiple Investor Identifiers" matching 3+ investor names from the dictionary (lower threshold than the client variant because any multi-investor document is already concerning)
- DLP rule: Block external sharing, block copy to any non-approved destination, require justification for all internal sharing outside the IR team, audit all access with high-severity logging
- Mode: Enforce

C.4 Advanced audit retention

What it catches: Not a DLP rule per se, but an enabling configuration for every other rule's forensic value.

Why it's here: FSA examinations can look back years. Standard Purview audit retention is 180 days, which is not sufficient for regulatory defense. FSA-regulated clients should have Advanced Audit enabled with 10-year retention on all DLP-related events.

Configuration:

- Purview → Settings → Audit → verify Advanced Audit is enabled (requires E5 licensing)
- Purview → Audit → Retention policies → Create → retain DLP events and file access events for 10 years
- Document the retention policy in the client's compliance documentation
- Include audit log export to cold storage as a quarterly operational task

C.5 Communication compliance for investment discussions

What it catches: Teams messages, emails, and meeting transcripts discussing investment decisions, recommendations, or client positions in ways that violate compliance policy.

Why it's here: FSA rules require supervision of communications relating to investment recommendations. This is a Communication Compliance use case rather than DLP strictly, but the content classification underlies both.

Configuration:

- Purview → Communication Compliance → Policies → Create
- Template: Sensitive info types with a custom classifier for investment terminology in Japanese and English
- Monitored scope: Trading team, research team, client-facing advisors
- Review queue: Compliance team

- Mode: Audit with sampling (review 5% of matches) initially, scale based on findings

Deployment approach

Regardless of which overlay you're deploying, follow this sequence. It exists because deploying DLP in one big bang creates visible disruption that damages the project's credibility and makes tuning impossible.

Phase 1: Audit mode (weeks 1-2)

Deploy every rule in audit mode with no user notifications. Watch Activity Explorer for matches. The goal is to understand what the rules catch in the client's actual environment before anything visible happens to end users.

Expected outcomes: you'll discover false positives, legitimate business processes that the rules interfere with, and gaps in your content classification (content that should match but doesn't). All of these are normal findings and get addressed before Phase 2.

Phase 2: Notify mode (weeks 3-4)

Turn on user notifications for rule matches, still without blocking. Users start seeing "this action triggered a DLP rule" messages. The goal is to train user behavior and surface legitimate use cases that need exceptions.

Expected outcomes: a wave of user questions ("why did I get this notification when I was just emailing my colleague?"), some legitimate exception requests, and a general increase in awareness that DLP exists. Handle the questions promptly — tone-set for the deployment.

Phase 3: Enforce (week 5+)

Turn on blocking for rules where blocking is configured. Keep audit-only for rules that are informational.

Expected outcomes: a small number of blocked actions, user escalations for genuine business needs that weren't captured in earlier phases, and the beginning of steady-state operation.

Phase 4: Steady state (ongoing)

Monthly review of Activity Explorer, quarterly review of policy effectiveness with the client, annual review of the full baseline against changes in client business and Microsoft feature updates.

Tuning and exception handling

Every baseline deployment will need client-specific tuning. Common adjustments:

- **Exclude the client's own documentation SharePoint site** from credential detection rules (they have example credentials in docs)
- **Add allowlist entries** for the client's approved cloud services so upload-to-cloud rules don't fire on legitimate uploads to their own file sharing
- **Add exception groups** for users with legitimate access to sensitive content (Finance team for financial data rules, Legal team for contract templates)
- **Adjust match thresholds** in keyword dictionary SITs based on observed false positive rates
- **Create client-specific sensitive info types** for their unique identifiers (internal project codes, product names, employee ID formats)

All tuning should be documented in the client's DLP implementation log, kept alongside their tenant documentation. Future eSolia staff need to understand why a given exception exists.

What’s deliberately not in the baseline

A few policies are common in Purview deployments but are deliberately not part of the eSolia baseline. Knowing why is important because clients sometimes ask for them.

Full email content scanning with keyword matching. High false positive rate, low value, annoying for users. Only deploy when specifically requested and justified.

Block all external email with attachments. Creates too much friction to be sustainable. Users route around it via personal email, which is worse than the original risk.

Watermarking of all documents. Available through sensitivity labels but rarely useful and often ugly. Only deploy when there’s a specific requirement.

Trainable classifier for “company confidential” style content. The built-in trainable classifiers for generic business confidential content are unreliable. Use sensitivity labels and explicit SITs instead.

Block access to all personal cloud storage. Better handled at the network layer (Cloudflare Zero Trust, firewall DNS filtering) than at the DLP layer. DLP policies for this purpose fire too late in the workflow.

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