Sensitivity Label Taxonomy and Application Guide

秘密度ラベル分類体系・適用ガイド

April 11, 2026 / 2026 年 4 月 11 日

English Version

See page 12 →

日本語版

3 ページへ →

eSolia

秘密度ラベル分類体系・適用ガイド

2026 年 4 月 11 日

目次

> eSolia INTERNAL — 本ドキュメントは、Microsoft Purview 秘密度ラベルを通じて運用される eSolia の情報分類体系を説明するものです。

正本: Microsoft Purview コンプライアンスポータル。本ドキュメントは人間が読める解説書であり、相互参照用です。分類体系が変更された場合は、Purview から再構築してください（四半期ごとのレビュー）。

ISO 27001 対応: 本分類体系は ISO 27001:2022 附属書 A 管理策 A.5.12（情報の分類）、A.5.13（情報のラベル付け）、A.8.10（情報の削除/分類に基づく取扱い）の要件を実装しています。

第 1 層: 分類体系

eSolia では 7 段階の秘密度ラベルを使用しています。優先度 0（最も制限が少ない）から優先度 6（最も制限が厳しい）まで順に並んでいます。競合が発生した場合、高い優先度のラベルが優先されます。

ラベル一覧表

優先度	表示名	EN 表示名	用途
0	社外一般	Public	保護不要
1	業務共有	Work Share	通常の社外共有
2	商用書類	Commercial Papers	顧客向けビジネス文書
3	社内一般	Protected Internal	社内限定、基本的な保護
4	顧客機密情報	Client Confidential	注意義務下の顧客データ
5	秘密	Confidential	機密性の高い社内情報（人事、契約）
6	極秘	Restricted	最高分類（財務、経営戦略）

各ラベルの詳細定義

0. Public 社外一般

適用場面: 社外一般にアクセス可能な資産。漏洩した場合に、影響がないもの。

例: パンフレット、一般プレゼンテーション、ウェブサイトページ、マーケティング資料

項目	設定値
スコープ	ファイル・データ資産、メール、PurviewAssets
アクセス制御	なし
コンテンツマーキング	なし
自動ラベル	なし

注意: ラベルなし＝パブリックではありません。ラベルがないことは、ユーザーがまだ分類していないことを意味します。「Public」の適用は、開示しても問題ないという意思表示です。

1. Work Share 業務共有

適用場面: 通常業務の過程で社外の特定人物と共有するコンテンツ。内容自体は機密ではないが、不注意な転送は軽微な影響を及ぼす可能性あり。

例: 顧客との業務に関するメール、会議の日程調整、機密性のないプロジェクト連絡

項目	設定値
スコープ	ファイル・データ資産、メール
アクセス制御	なし
コンテンツマーキング	なし
自動ラベル	なし

2. Commercial Papers 商用書類

適用場面: 顧客先の特定人物と共有する書類で、顧客による処理が必要なもの。漏洩した場合は顧客にとってマイナスな影響を受ける可能性あり。

例: 見積書、概算見積、請求書、納品書、レポート、契約書、Hanawa CMS で生成した提案書

項目	設定値
スコープ	ファイル・データ資産、メール
アクセス制御	なし
コンテンツマーキング	なし
自動ラベル	なし

3. Protected Internal 社内一般

適用場面: 社員及び承認されたスタッフのみが利用する社内コンテンツ。社内限定ラベルの中で最も制限が緩い。社外の人間の目に付く場所に置いてはならない。

例: 会議の議事録、顧客リスト、営業企画書、社内 SOP、チームドキュメント

項目	設定値
スコープ	ファイル・データ資産、メール、会議、サイト、M365 グループ、PurviewAssets
アクセス制御	なし
コンテンツマーキング	フッター: `Protected Internal 社内一般`
自動ラベル	なし

下位ラベルとの違い: コンテンツマーキング（フッター）が付く最初のラベルです。Teams 会議、SharePoint サイト、M365 グループにも適用可能です。

4. Client Confidential 顧客機密情報

適用場面: 顧客から受け取った、またはサービスの提供過程で顧客のために作成した文書及び情報。アクセスは、その顧客のサポートに直接関与するチームに限定。

例: ネットワーク図面・ラック図面、フロアプラン、ユーザーリスト、セキュリティ評価、顧客の書類、システム設定エクスポート

項目	設定値
スコープ	ファイル・データ資産、メール、会議、サイト、M365 グループ、PurviewAssets
アクセス制御	なし
コンテンツマーキング	なし
自動ラベル	なし

重要な区別: Client Confidential（優先度 4）は Protected Internal（優先度 3）より上位です。これは、漏洩が eSolia だけでなく顧客に損害を与えるためです。**別の顧客に見られたくない情報**には、このラベルを適用してください。

5. Confidential 秘密

適用場面: 役員やプロジェクトに携わっている人など、一部の人のみが閲覧を認められる文書。Protected Internal より重要度が高く、人事・法務・重要契約情報が該当。

例: 重要契約書、人事ファイル、顧客システム認証情報、給与情報、法務書簡、インシデント対応報告書

項目	設定値
スコープ	ファイル・データ資産、メール、会議、サイト、M365 グループ、PurviewAssets
アクセス制御	なし
コンテンツマーキング	フッター: `Confidential 秘密`
自動ラベル	有効（Purview が機密情報タイプを検出し自動適用）

自動ラベル: 自動適用が有効な唯一のラベルです。Purview が日本固有の PII（マイナンバーパターン等）や財務データパターンを検出して自動適用します。定期的に自動ラベル付与の精度を確認してください。

6. Restricted 極秘

適用場面: 最高分類。企業経営に直結する内容（財務、経営戦略等）で、漏洩が長期的な戦略目標に深刻な影響を与える、または組織の存続を危険にさらすもの。経営に関わる役員などごく一部の人だけがアクセス可能。

例: 特命プロジェクト、未公開の経理情報、M&A 関連、法定届出書類、取締役会決議、セキュリティインシデントフォレンジック

項目	設定値
スコープ	ファイル・データ資産、メール、会議、サイト、M365 グループ、PurviewAssets
アクセス制御	なし
コンテンツマーキング	フッター: `Restricted 極秘`
自動ラベル	なし

保護設定サマリー

ラベル	優先度	フッター	暗号化	自動ラベル	グループ/サイト/会議
Public 社外一般	0	なし	なし	なし	なし
Work Share 業務共有	1	なし	なし	なし	なし
Commercial Papers 商用書類	2	なし	なし	なし	なし
Protected Internal 社内一般	3	あり	なし	なし	あり
Client Confidential 顧客機密情報	4	なし	なし	なし	あり
Confidential 秘密	5	あり	なし	あり	あり
Restricted 極秘	6	あり	なし	なし	あり

現状（2026 年 4 月）: 暗号化やアクセス制御を強制するラベルはありません。現在は分類+コンテンツマーキング+ユーザー意識で運用中です。暗号化の強制は今後の強化項目です（運用メモ参照）。

第 2 層: 判断ガイド — どのラベルを適用すべきか

迷ったときは、以下の質問を順に確認してください。

判断テーブル

確認事項	該当する場合の適用ラベル
公開ウェブサイトに掲載しても問題ないか?	**Public 社外一般**
顧客との通常業務のやり取りか?	**Work Share 業務共有**
顧客に送る正式なビジネス文書（見積書、請求書、契約書）か?	**Commercial Papers 商用書類**
社内限定だが、特に機密性はないか?	**Protected Internal 社内一般**
顧客から受け取った、または顧客のために作成した情報か?	**Client Confidential 顧客機密情報**
人事データ、給与情報、法務事項、重要契約が含まれるか?	**Confidential 秘密**
漏洩が会社の存続や戦略的地位を脅かすか?	**Restricted 極秘**

よくあるシナリオ

シナリオ	ラベル	理由
顧客との会議日程調整メール	Work Share	通常のやり取り、影響は軽微
顧客に送る SOW・提案書	Commercial Papers	顧客処理を要する正式文書
社内チームの Wiki ページ	Protected Internal	社内参照用、機密性なし
顧客の AD ユーザーエクスポート	Client Confidential	サービス提供中に作成した顧客データ
社員の人事評価書	Confidential	人事データ、アクセス限定
顧客 DC のネットワーク図面	Client Confidential	顧客のために作成
eSolia 自社の年次決算書（ドラフト）	Restricted	未公開の財務情報
esolia.co.jp 向けブログ記事のドラフト	Public	公開予定のコンテンツ
顧客のセキュリティインシデント報告書	Client Confidential	顧客データ、機密コンテキスト
eSolia 社員の給与一覧	Confidential	人事/財務、社内
オフィス移転に関する取締役会決議	Restricted	経営戦略上の決定

2 つのラベルが該当しそうな場合

優先度が高い方を適用します。例:

- 顧客納品物（Commercial Papers）に顧客のネットワーク図面（Client Confidential）が含まれる場合: **Client Confidential**（優先度 4 > 2）

- 議事録（Protected Internal）に給与交渉の内容（Confidential）が含まれる場合: **Confidential**（優先度 5 > 3）
- 顧客契約書（Commercial Papers）に eSolia の価格戦略（Restricted）が含まれる場合: **Restricted**（優先度 6 > 2）

「顧客データ」ルール

顧客から受領した、または顧客環境のために作成した情報は、内容がどれほど日常的に見えても、**最低でも Client Confidential** です。顧客のオフィスフロアプランは一見何気ないものに見えますが、それは顧客の情報であり、eSolia には注意義務があります。

「ラベルなし ≠ パブリック」ルール

ラベルのないコンテンツは「未分類」であり、暗黙的にパブリックではありません。SharePoint や Teams でラベルのないコンテンツを見つけた場合は、適切なラベルを適用してください。「Public」の適用は、内容を評価した上で開示に問題がないと判断した意思表示です。

第 3 層: 運用メモ

自動ラベル設定

自動ラベルが有効なのは **Confidential 秘密**（優先度 5）のみです。Purview のトレーナブル分類子および機密情報タイプが以下のパターンを検出します:

- 日本固有の PII（マイナンバーパターン等）
- 財務データパターン
- 人事関連の文書構造

自動ラベル付与された文書は定期的にレビューしてください。自動ラベルはセーフティネットであり、手動分類の代替ではありません。

Purview 設定の既知の問題

内部名と表示名の入れ替わり: 2 つのラベルで、Purview 内部名と表示名の日本語が入れ替わっています:

ラベル	Purview 内部名	表示名（ユーザーに表示）
Confidential	Confidential **極秘**	Confidential **秘密**
Restricted	Restricted **秘密**	Restricted **極秘**

表示名が正しい設定です（極秘は秘密より厳格で、Restricted の最高優先度に対応）。内部名は逆になっています。ユーザーは Office アプリで表示名を見るため機能的な影響はありませんが、Purview 管理画面や CSV エクスポートで混乱を招く可能性があります。

ラベルスコープの差異

ラベル 0-2（Public、Work Share、Commercial Papers）はラベル 3-6 よりスコープが狭い:

- **0-2 に不足:** 会議、サイト、M365 グループ
- **影響:** Public、Work Share、Commercial Papers を Teams チャンネル、SharePoint サイト、M365 グループに適用できない
- **回避策:** パブリックコンテンツをホストする SharePoint サイトには、サイトコンテナに Protected Internal を適用し、個々のファイルに Public を適用

暗号化ロードマップ

現在、暗号化を強制するラベルはありません。計画中の段階的導入:

1. **現在（2026 Q2）:** 分類+コンテンツマーキングのみ
2. **計画中（2026 Q3-Q4）:** Confidential と Restricted に暗号化を追加
3. **将来:** Client Confidential への暗号化を検討（複雑性: 顧客がドキュメントを開ける必要がある）

ラベルの肥大化防止

7 つのラベルは、ユーザーが確実に区別できる上限に近い数です。新しいラベルを追加する前に:

1. 既存のラベルで対応できないか? 新規作成より再利用を優先。
2. 新しいラベルに異なる技術的保護（暗号化、DLP ルール）が必要か? 不要なら、それは別のラベルではなく、命名規則やメタデータで対応すべきサブカテゴリ。
3. 全スタッフの再研修が必要か? 組織的コストを考慮。

絶対ルール: ISMS の委員会による明示的な承認なしに 10 ラベルを超えてはならない。

四半期レビュープロセス

毎四半期（1 月、4 月、7 月、10 月）、ISMS 管理者は以下を実施:

1. Purview から現在のラベル設定をエクスポート（Settings > Sensitivity labels > Export to CSV）
2. 本ドキュメントとの差異を確認
3. 自動ラベルの精度をレビュー（自動ラベル付与文書のサンプルチェック）
4. 高機密性 SharePoint サイトのラベルなしコンテンツを確認
5. 分類体系に変更があれば本ドキュメントを更新
6. ISMS 監査ログにレビューを記録

ラベルの廃止プロセス

ラベルを廃止する場合:

1. 対象ラベルが付与された全コンテンツを特定（Purview Content Explorer）
2. コンテンツを適切な後継ラベルに再ラベル付与
3. Purview でラベルを「Disabled」に設定（削除しない。監査証跡を保持）
4. 90 日間の移行期間後、Office アプリのラベルピッカーから削除
5. 本ドキュメントおよび Hanawa CMS の秘密度ドロップダウンを更新

eSolia

Sensitivity Label Taxonomy and Application Guide

April 11, 2026

Contents

> eSolia INTERNAL — This document describes eSolia's information classification system enforced through Microsoft Purview sensitivity labels.

Source of truth: Microsoft Purview compliance portal. This document is the human-readable explanation and cross-reference. Rebuild from Purview when the taxonomy changes (quarterly review).

ISO 27001 alignment: This taxonomy implements the requirements of ISO 27001:2022 Annex A controls A.5.12 (Classification of information), A.5.13 (Labelling of information), and A.8.10 (Information deletion / handling by classification).

Layer 1: The Taxonomy

eSolia uses 7 sensitivity labels, ordered from least restrictive (priority 0) to most restrictive (priority 6). Higher priority labels override lower ones when conflicts arise.

Label Reference Table

Priority	Display Name	JA Display	Purpose
0	Public	社外一般	No protection needed
1	Work Share	業務共有	Routine external sharing
2	Commercial Papers	商用書類	Client-facing business documents
3	Protected Internal	社内一般	Internal-only, baseline protection
4	Client Confidential	顧客機密情報	Client data under duty of care
5	Confidential	秘密	Sensitive internal (HR, contracts)
6	Restricted	極秘	Highest classification (financials, strategy)

Detailed Label Definitions

0. Public 社外一般

When to apply: Content intended for the general public where disclosure causes no harm.

Examples: Pamphlets, general presentations, website pages, marketing collateral.

User description (as shown in Office apps):

> Assets that can be viewed by the general public, for which disclosure causes no harm. Examples: pamphlets, general presentations, website pages

Property	Value
Scope	Files & other data assets, Email, PurviewAssets
Access control	None
Content marking	None
Auto-labeling	None

Note: Unlabeled content does not automatically mean public. The absence of a label means the user has not yet classified the content. Applying "Public" is an affirmative statement that disclosure is acceptable.

1. Work Share 業務共有

When to apply: Content shared with specific external individuals in the course of normal business operations. The content itself is not sensitive, but careless forwarding could cause minor impact.

Examples: Routine work emails with clients, meeting scheduling, non-sensitive project coordination.

User description:

> Items that are shared with specific people outside the organization. If disclosed, there may be a negative impact so care is needed, especially with regard to forwarding. Examples: typical work emails with clients

Property	Value
Scope	Files & other data assets, Email
Access control	None
Content marking	None
Auto-labeling	None

2. Commercial Papers 商用書類

When to apply: Business documents shared with specific client contacts that require processing by them. Disclosure could negatively impact the client relationship.

Examples: Quotes, estimates, invoices, delivery notes, reports, contracts, proposals generated via Hanawa CMS.

User description:

> Commercial papers that are shared outside the organization with specific individuals at clients, requiring processing by them. If disclosed, there may be a negative impact from the client's perspective, so care is needed, especially with regard to forwarding.

Property	Value
Scope	Files & other data assets, Email
Access control	None
Content marking	None
Auto-labeling	None

3. Protected Internal 社内一般

When to apply: Content for internal use by employees and authorized staff only. This is the baseline internal classification — the least restrictive of the internal-only labels. Content must not be placed where external parties can view it.

Examples: Meeting minutes, customer lists, sales plans, internal SOPs, team documentation.

User description:

> Protected or internal assets available for general internal access to employees or specific staff. Besides public, this is the least strict classification, and care must be taken not to place so labeled assets where people outside the company can view them.

Property	Value
Scope	Files & other data assets, Email, Meetings, Site, UnifiedGroup, PurviewAssets
Access control	None
Content marking	Footer: `Protected Internal 社内一般`
Auto-labeling	None

Key difference from lower labels: This is the first label with content marking (footer). It also has the broadest scope, applying to Teams meetings, SharePoint sites, and Microsoft 365 groups in addition to files and email.

4. Client Confidential 顧客機密情報

When to apply: Client information received from or created for a client during service delivery. Access is restricted to the team directly involved in supporting that client.

Examples: Network or rack diagrams, floor plans, user lists, security assessments, client documentation, system configuration exports.

User description:

> Client Confidential information or documents are limited in access to the team directly involved in supporting the client, and should be handled with due care. This is applied to documents and information received from the client or created for the client in the course of delivering service.

Property	Value
Scope	Files & other data assets, Email, Meetings, Site, UnifiedGroup, PurviewAssets
Access control	None
Content marking	None
Auto-labeling	None

Important distinction: Client Confidential (priority 4) is higher than Protected Internal (priority 3) because disclosure harms the client, not just eSolia. The duty of care is external. Apply this label to anything you would not want a different client to see.

5. Confidential 秘密
When to apply: Sensitive internal documents accessible only to directors or staff involved in specific projects. More restrictive than Protected Internal. Covers HR, legal, and significant contractual information.

Examples: Important contracts, personnel files, client system credentials, salary information, legal correspondence, incident response reports.

User description:

> Confidential documents are limited in access to company directors or staff involved in specific projects. This is a heavier classification than the “internal protected” document, and is applied to HR or contract information.

Property	Value
Scope	Files & other data assets, Email, Meetings, Site, UnifiedGroup, PurviewAssets
Access control	None
Content marking	Footer: `Confidential 秘密`
Auto-labeling	Automatic (Purview auto-applies based on sensitive information types)

Auto-labeling: This is the only label with automatic application enabled. Purview detects sensitive information types (Japan-specific PII, financial data patterns) and applies this label automatically. Review auto-labeled content periodically to verify accuracy.

6. Restricted 極秘

When to apply: The highest classification. Content directly related to company financials, strategic plans, or matters where disclosure would have serious impact on long-term objectives or put the survival of the organization at risk. Access limited to directors involved in statutory matters.

Examples: Critical strategic projects, unpublished financials, M&A activity, statutory filings, board-level decisions, security incident forensics.

User description:

> Restricted documents are of critical importance, and are subject to the strictest administration standard, related directly to company financials or plans. Access is limited to company directors involved directly in statutory matters.

Property	Value
Scope	Files & other data assets, Email, Meetings, Site, UnifiedGroup, PurviewAssets
Access control	None
Content marking	Footer: `Restricted 極秘`
Auto-labeling	None

Protection Summary Matrix

Label	Priority	Footer	Encryption	Auto-label	Groups/Sites/ Meetings
Public	0	No	No	No	No
Work Share	1	No	No	No	No
Commercial Papers	2	No	No	No	No
Protected Internal	3	Yes	No	No	Yes
Client Confidential	4	No	No	No	Yes
Confidential	5	Yes	No	Yes	Yes
Restricted	6	Yes	No	No	Yes

Current state (April 2026): No labels enforce encryption or access control. Protection is currently classification + content marking + user awareness. Encryption enforcement is a planned enhancement (see Operational Notes).

Layer 2: Decision Guidance — Which Label Should I Apply?

This is the section that matters most. If you are unsure which label to apply, work through these questions in order.

Quick Decision Table

Ask yourself···	If yes, apply···
Would I put this on our public website?	**Public 社外一般**
Am I sharing this with a client contact as routine work correspondence?	**Work Share 業務共有**
Is this a formal business document (quote, invoice, contract) going to a client?	**Commercial Papers 商用書類**
Is this for internal use only, but not particularly sensitive?	**Protected Internal 社内一般**
Did I receive this from a client, or did I create it for a specific client's environment?	**Client Confidential 顧客機密情報**
Does this contain HR data, salary info, legal matters, or sensitive contracts?	**Confidential 秘密**
Would disclosure of this threaten the company's survival or strategic position?	**Restricted 極秘**

Common Scenarios

Scenario	Label	Why
Email to client about scheduling a meeting	Work Share	Routine correspondence, minimal impact
SOW or proposal sent to client	Commercial Papers	Formal document requiring client processing
Internal team wiki page	Protected Internal	Internal reference, not sensitive
Client's Active Directory user export	Client Confidential	Client data created during service delivery
Employee performance review	Confidential	HR data, limited access
Network diagram you drew for client's DC	Client Confidential	Created for client during service
eSolia's own annual financial statements (draft)	Restricted	Unpublished financials
Blog post draft for esolia.co.jp	Public	Intended for publication
Incident response report for a client breach	Client Confidential	Client data, sensitive context
eSolia staff salary spreadsheet	Confidential	HR/financial, internal
Board resolution on office relocation	Restricted	Strategic decision, director-level

When Two Labels Seem Right

Apply the **higher-priority** label. Examples:

- A document is both a client deliverable (Commercial Papers) and contains client network diagrams (Client Confidential): apply **Client Confidential** (priority 4 > 2).
- Meeting minutes (Protected Internal) that discuss salary negotiations (Confidential): apply **Confidential** (priority 5 > 3).
- A client contract (Commercial Papers) that includes eSolia pricing strategy (Restricted): apply **Restricted** (priority 6 > 2).

The “Client Data” Rule

If information originated from a client or was created specifically for a client’s environment, it is **at minimum Client Confidential**, regardless of how routine the content seems. A client’s office floor plan may seem mundane, but it is their information and eSolia has a duty of care.

The “Unlabeled Is Not Public” Rule

Content without a label has not been classified. It is not implicitly public. If you encounter unlabeled content in SharePoint or Teams, apply the appropriate label. Applying “Public” is an affirmative decision — it means you have evaluated the content and determined that disclosure causes no harm.

Layer 3: Operational Notes

Auto-Labeling Configuration

Only **Confidential 秘密** (priority 5) has auto-labeling enabled. Purview's trainable classifiers and sensitive information types detect patterns such as:

- Japan-specific PII (My Number patterns)
- Financial data patterns
- HR-related document structures

Auto-labeled documents should be reviewed periodically. Auto-labeling is a safety net, not a substitute for manual classification.

Known Purview Configuration Issues

Name vs. Display Name swap: Two labels have mismatched internal names and display names in Purview:

Label	Internal Name (Purview)	Display Name (shown to users)
Confidential	Confidential **極秘**	Confidential **秘密**
Restricted	Restricted **秘密**	Restricted **極秘**

The Display Names are correct (極秘 is stricter than 秘密, matching Restricted's highest priority). The internal Names are backwards. This has no functional impact — users see Display Names in Office apps — but may cause confusion when viewing Purview admin screens or CSV exports.

Label Scope Gaps

Labels 0-2 (Public, Work Share, Commercial Papers) have narrower scope than labels 3-6:

- **Missing from 0-2:** Meetings, Site, UnifiedGroup
- **Impact:** You cannot apply Public, Work Share, or Commercial Papers to Teams channels, SharePoint sites, or Microsoft 365 groups. Only files and emails.
- **Workaround:** If a SharePoint site hosts public content, apply Protected Internal to the site container and Public to individual files.

Encryption Roadmap

No labels currently enforce encryption. The planned progression:

1. **Current (2026 Q2):** Classification + content marking only
2. **Planned (2026 Q3-Q4):** Add encryption to Confidential and Restricted
3. **Future:** Evaluate encryption for Client Confidential (complexity: client recipients need to be able to open documents)

DLP Policy Integration

Current DLP policies reference sensitivity labels for Endpoint DLP on managed devices. DLP rules that trigger on labels:

- **Endpoint DLP:** Monitors copy/paste and file transfer actions on labeled documents (requires Defender for Endpoint + DLP feature flag enabled)
- **Exchange DLP:** Not yet configured per-label

- **SharePoint DLP:** Not yet configured per-label

Label Sprawl Prevention

Seven labels is already at the upper bound of what users can reliably distinguish. Before adding a new label:

1. Can the use case be handled by an existing label? Prefer reusing over creating.
2. Does the new label require different technical protection (encryption, DLP rules)? If not, it is not a distinct label — it is a subcategory that should be handled by naming conventions or metadata.
3. Would adding the label require retraining all staff? Factor the organizational cost.

Hard rule: Do not exceed 10 labels without explicit ISMS committee approval.

Quarterly Review Process

Every quarter (January, April, July, October), the ISMS manager should:

1. Export the current label configuration from Purview (Settings > Sensitivity labels > Export to CSV)
2. Compare against this document for drift
3. Review auto-labeling accuracy (check a sample of auto-labeled documents for false positives)
4. Check for unlabeled content in high-sensitivity SharePoint sites
5. Update this document if the taxonomy has changed
6. Record the review in the ISMS audit log

Retirement Process for Labels

If a label must be retired:

1. Identify all content bearing the label (Purview Content Explorer)
2. Re-label content to the appropriate replacement
3. Set the label to “Disabled” in Purview (do not delete — historical audit trail)
4. Remove from Office app label picker after a 90-day transition period
5. Update this document and the Hanawa CMS sensitivity dropdown