サポート情報記事

Policy Acknowledgement：ソリューションの概要

2026 © Vitextra SIA. 無断転載を禁じます。

免責事項

本免責事項の適用上、次のとおり定義します。

- **会社** (本免責事項では「当社」と表記します) とは、Vitextra SIA (Matīsa iela 61-25, Rīga, LV-1009, Latvia) を指します。
- **本ドキュメント**とは、ナレッジベースの記事を指します。
- **お客様**とは、本ドキュメントにアクセスする個人、または該当する場合は、その個人が本ドキュメントにアクセスまたは使用する際に代理となっている会社その他の法人を指します。
- **本 Web サイト**とは、https://vitextra.com からアクセスできる Vitextra を指します。

免責事項

本ドキュメントに記載されている情報は、一般的な情報提供のみを目的としています。

当社は、本ドキュメントの内容における誤りや脱漏について、一切責任を負いません。

いかなる場合も、契約上の訴訟、過失、その他の不法行為上の訴訟であるかを問わず、本ドキュメントの内容の使用に起因または関連して生じる、特別損害、直接損害、間接損害、結果的損害、付随的損害、またはその他一切の損害について、当社は責任を負いません。当社は、事前の通知なく、いつでも本ドキュメントの内容に追加、削除、または変更を行う権利を留保します。

誤りおよび脱漏に関する免責事項

本ドキュメントに記載されている情報は、関心のある事項に関する一般的な指針を示すことのみを目的としています。そのため、本ドキュメントの内容を最新かつ正確に保つために当社があらゆる予防措置を講じている場合でも、誤りが生じる可能性があります。また、法律、規則、規制は変化するため、本ドキュメントに記載されている情報に遅れ、脱漏、または不正確な点が含まれる場合があります。

当社は、誤りや脱漏、またはこの情報の使用によって得られた結果について、責任を負いません。

フェアユースに関する免責事項

当社は、著作権者から明示的な許可を得ていない著作物を使用する場合があります。当社は、批評、論評、ニュース報道、教育、学術研究、または調査の目的で、そのような資料を提供しています。

当社は、これが、米国著作権法第 107 条に規定されている、当該著作物の「フェアユース」にあたると考えています。

お客様が、フェアユースの範囲を超えて、ご自身の目的で本ドキュメントの著作物を使用することを希望される場合は、著作権者から許可を得る必要があります。

「自己責任での使用」に関する免責事項

本ドキュメントのすべての情報は、完全性、正確性、適時性、またはこの情報の使用によって得られる結果について何ら保証することなく、また、性能、商品性、特定目的への適合性に関する保証を含むがこれらに限定されない、明示または黙示を問わずいかなる種類の保証もなく、「現状のまま」提供されます。

当社は、本ドキュメントに記載されている情報に依拠して行われた判断や措置、または結果的損害、特別損害、もしくはこれらに類する損害について、たとえそのような損害の可能性について知らされていた場合でも、お客様またはその他の者に対して責任を負いません。

お問い合わせ

本免責事項についてご不明な点がある場合は、メール (support@vitextra.com) でお問い合わせください。

目次

このソリューションで管理できること 4

ワークフローを構成するオブジェクト 4

担当者ごとの役割 5

下書きから確認までの流れ 6

適切な**Web**パーツを選ぶ 6

コンテンツ、バージョン、閲覧条件 8

進捗と証跡を理解する 8

導入と動作モード 9

最初の導入を成功させるために 9

Policy Acknowledgementは、従業員への社内ポリシーの配布と、読んだことの確認記録を管理するVitextraのソリューションです。SharePoint Online上でポリシーカタログ、管理された公開、従業員への割り当て、管理レポートを結び付けます。従業員は専用ページで自分の作業を確認し、ポリシーを読み、質問し、確認を送信します。個人用のMy Policiesアプリを Microsoft Teamsでの入口として使うこともできます。

ライブラリに文書を保存するだけでは不十分な場合に役立ちます。適用するバージョン、配布先、回答期限、未完了の作業をどうフォローするかを決める必要があるためです。たとえば、試験導入の部門にセキュリティポリシーを割り当て、後から重要な改訂を公開して、その更新による割り当てを初回リリースとは別に追跡できます。

このソリューションで管理できること

代表的な用途は、特定の従業員グループへの社内ポリシーの導入、重要な変更後の確認依頼、チームで未完了のポリシーの確認、従業員が確認文に同意できない理由の調査です。必須の個人割り当てと並行して、閲覧可能なカタログを維持できます。ポリシーを読めることは、必ずしも確認が割り当てられていることを意味しません。

グループと従業員属性に基づく対象者ルールをサポートしています。ポリシー所有者は、キャンペーンごとに別の手作業のスプレッドシートを管理せずに、業務上の対象者を選択できます。個別の追加と除外で例外に対応し、対象者プレビューで割り当て作成前に確認できます。

定期キャンペーンや常時実行キャンペーンの選択肢がありますが、その名称だけで完全なバックグラウンド処理が動作していると判断しないでください。その後の対象者更新、スケジュールされたリマインダー、エスカレーションには別のサービスコンポーネントが必要です。現在の実装では、同じバージョンの割り当ての重複防止も再確認を制限します。

ワークフローを構成するオブジェクト

オブジェクト	表すもの	役割
ポリシー	タイトル、所有者、カテゴリ、ソース、日付、閲覧条件を持つカード。	ポリシー管理を、その本文が入ったファイルやページから分離します。

オブジェクト	表すもの	役割
バージョン	番号、変更の説明、対応する場合はフィンガープリントとスナップショットを持つ公開リリース。	キャンペーンと確認に関連するリリースを特定します。
キャンペーン	対象者と期限設定を持つポリシーバージョンの配布。	特定の割り当て操作を定義します。
割り当て	ポリシーバージョンとキャンペーンに対する、ある従業員の作業項目。	期限、状態、関連する確認を追跡します。
確認	記録された確認、または別の証跡イベント。	確認文、本人情報、時刻、関連する技術的証跡を保持します。
質問	従業員の質問、または確認できない理由。	所有者に例外解決のための作業キューを提供します。

バージョンの公開と割り当ての作成は別の操作です。初回公開はリリースを利用可能にしますが、キャンペーンを自動開始しません。同様に、ライブラリでコンテンツを開いても、割り当ての作成や確認の記録は自動的には行われません。

担当者ごとの役割

管理者はストレージ、ロール、サービス設定を構成します。コンプライアンス管理者は製品全体のポリシーとキャンペーンを管理し、免除を判断します。作成者はポリシーを作成し、自分が所有するカードを扱います。監査担当者はレポートビューを利用します。従業員は割り当てを受け取り、上司は配下のチームを確認します。

ロールのグループはPolicy Adminで集中管理します。ポリシー所有者は別のフィールドであり、変更すると作成者に見える内容が変わることがあります。報告階層はディレクトリの関係から取得され、ロール割り当て一覧で手作業管理する第六

のロールではありません。製品ロールは、SharePointページの編集やアプリの展開権限を自動的に与えるものではありません。

下書きから確認までの流れ

1 ハブを準備し、従業員用と管理用のページを接続します。
2 ポリシーカードを作成して所有者を設定し、文書、SharePointページ、外部URLのいずれかをソースに選びます。
3 確認文と必要な閲覧条件を設定し、最初のバージョンを公開します。
4 キャンペーンを作成し、対象者を確認して確認期限を指定します。
5 試験導入の従業員に、割り当てを開き、内容を読んで確認を送信してもらいます。
6 キャンペーンの対象者を広げる前に、従業員の受領書とレポートの結果を確認します。

たとえば、ポリシー所有者は架空の情報セキュリティポリシーを小規模なグループにまず割り当てられます。従業員が確認文に同意できない場合は、代わりに理由を提示できます。ケースはレビューに回され、権限のあるユーザーが回答、割り当ての再開、理由付きの免除記録を行えます。免除は、従業員に代わって確認する操作ではありません。



従業員ビューは個人の作業とポリシーの検索をまとめます

適切なWebパーツを選ぶ

Webパーツ	主な利用者	利用者ができること
My Policies	従業員	未完了の作業、期限、完了した確認、免除を確認します。

Webパーツ	主な利用者	利用者ができること
Policy Reader	従業員	ソースを読み、設定された条件を満たし、確認文を承認し、質問して受領書を表示します。
Policy Library	ポリシー閲覧者	公開済みおよびレビュー中のポリシーをカテゴリ別に閲覧し、メタデータを検索します。
Pending Policies Bar	イントラネット閲覧者	割り当て済みと期限超過のポリシーに関する簡潔な案内を見て、該当ページを開きます。
Policy Manager	所有者またはコンプライアンス担当チーム	ポリシーの作成と公開、キャンペーン開始、バージョン確認、従業員の質問対応を行います。
Compliance Dashboard	レポート利用者	指標、部門比較、過去日付の計算、エクスポート、証跡整合性の結果を調べます。
Team Compliance	上司	従業員ごとのポリシー状態を確認し、期限超過の割り当てに手動リマインダーを送ります。
Policy Admin	管理者	セットアップを完了し、ロール、カテゴリ、文面、通知、ストレージチェック、ライセンス、監査ログを管理します。

ページは組織のナビゲーションに合わせて配置できます。共通の閲覧ページはURLでポリシーと割り当ての識別子を使い、他のWebパーツはそこにリンクします。ストレージ作成ではこれらすべてのページは作成されないため、ページ設定とナビゲーションのテストも導入の一部です。

コンテンツ、バージョン、閲覧条件

文書ソースはブラウザーやOfficeビューアーで表示できます。SharePointページは、そのコンテンツを読み取れる場合にインライン表示できます。外部URLは宛先サイトの動作に従って開かれるか埋め込まれます。ソースを選択してもアクセス権は付与されず、外部サイトが埋め込みを禁止している場合もあります。

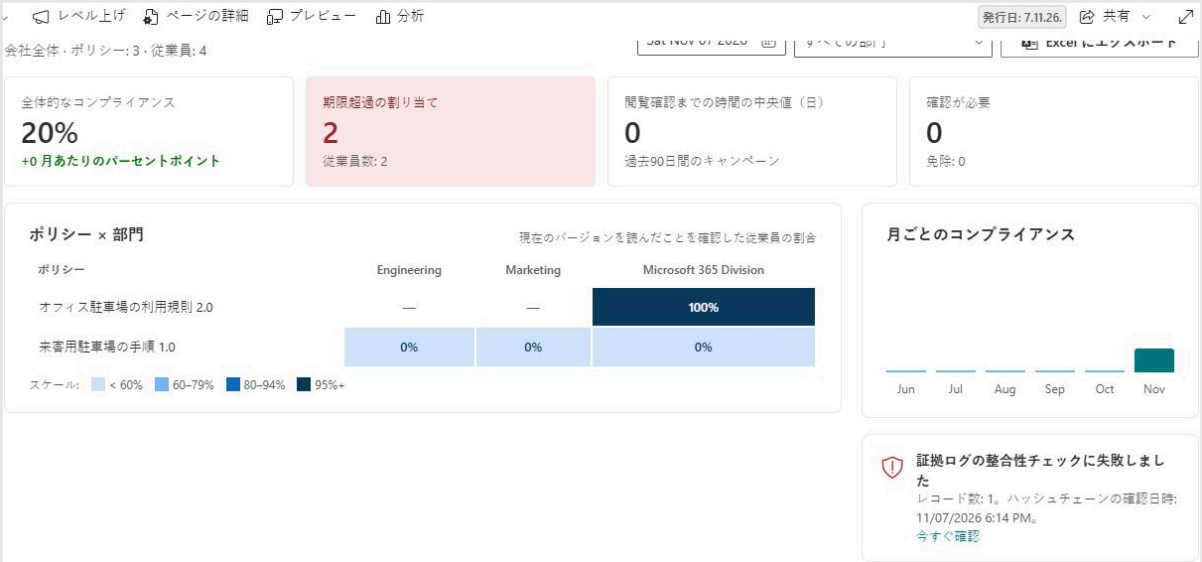
対応する同一オリジンの文書では、公開時にスナップショットを保存し、SHA-256フィンガープリントを計算します。ページと外部ソースのバージョンレコードには、それと同等のアーカイブ済みコンテンツのスナップショットはありません。現在のリーダーは、古い割り当ての保存済みスナップショットに自動で切り替えず、設定されたソースを表示します。アーカイブ済み文書バージョンを調べる際は、明示的なスナップショットリンクを使ってください。

所有者は、開くこと、スクロール、最低時間、氏名の入力を要求できます。これらは完了条件であり、内容を理解した証拠ではありません。フレーム内のページ以外のコンテンツでは、開いて所定の時間待つことでスクロール条件を満たせます。記録された確認は電子署名ではありません。

進捗と証跡を理解する

My Policiesは従業員に個人用一覧を提供します。Team Complianceは上司にチーム向けのマトリックスを提供します。Compliance Dashboardは、許可されたポリシー範囲の割り当てを部門と日付のフィルター付きで集計します。これらは異なる問いに答えるビューであり、分母やバージョン範囲が異なることがあります。割合を相互に置き換えられるものと考えないでください。

確認の受領書は、ポリシー、バージョン、確認時刻、確認文、該当するハッシュを記録します。監査ログは管理とワークフローの操作を記録します。コンプライアンスのExcelエクスポートには割り当て行が含まれますが、すべての証跡フィールドや過去のすべての遷移を完全に出力するものではありません。



管理レポートは完了状況と未完了の作業を明らかにします

導入と動作モード

SPFxソリューションは、リストとバージョンライブラリを備えたSharePointハブサイトを使います。Microsoft　Graphが従業員、グループ、報告関係のデータを提供し、手動メールリマインダーを支えます。試験導入前に、展開の承認、ソースコンテンツへのアクセス、ロールグループ、ページ構成を準備してください。ライセンスは既存のVitextraライセンス手順で管理します。

Directモードは従業員のセッションで通常の確認を記録します。Serviceモードは別途接続したサービスに送信します。設定の切り替えは、そのサービスのインストールやSharePoint権限の自動再適用を行いません。自動通知の設定も、実行中のスケジューラーが存在することを意味しません。

警告

Directモードは従業員に割り当てと確認レコードへの書き込み権限を与えます。現在のロールマトリックスはリスト単位であり、Webパーツの所有者や従業員フィルターはレコード単位の分離ではありません。ハッシュチェーン検証は不整合を検出できますが、レコードを絶対に変更不能にはしません。権限同期は実行アカウントにフルコントロールを残すため、インターフェイスが示すServiceモードの強い保護の説明は、有効な権限と照合する必要があります。

最初の導入を成功させるために

KB10496. Policy Acknowledgement：クイックスタートガイドのクイックスタートから始め、KB10497. Policy Acknowledgement：要件と権限で要件を、KB10500. Policy Acknowledgementのロールと権限を設定する方法でアクセス設定を確認してください。試験導入の従業員が実際に開けるソースを選び、対象者を明確に限定し、成功する確認と、質問または確認できないケースの両方をテストします。

対象を広げる前に、レポートの結果と保存された証跡を調べ、基になるデータを誰が閲覧または変更できるか確認してください。記録モードと保護の制限はKB10509. Policy Acknowledgementのデータ保存：DirectモードとServiceモードを参照します。バックグラウンドサービスの動作は別の導入チェックとして扱ってください。Webパーツプロジェクトだけでは、環境内でスケジュール操作、サービス権限、通知配信が機能しているとは確認できません。