WISSENSDATENBANKARTIKEL

Password Vault. Lösungsübersicht

2026 © Vitextra SIA. Alle Rechte vorbehalten.

Haftungsausschluss

Für die Zwecke dieses Haftungsausschlusses:

- **Das Unternehmen** (in diesem Haftungsausschluss entweder als „das Unternehmen“, „wir“, „uns“ oder „unser“ bezeichnet) bezieht sich auf Vitextra SIA, LV-1009 Riga, Matīsa iela 61 – 25.
- **Dokument** verweist auf den Wissensdatenbank-Artikel.
- **Sie** sind die Person, die auf das Dokument zugreift, bzw. das Unternehmen oder eine andere juristische Person, in deren Namen eine solche Person auf das Dokument zugreift oder es nutzt.
- **Die Website** verweist auf Vitextra, zugänglich über https://vitextra.com

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen dienen nur der allgemeinen Information.

Das Unternehmen übernimmt keine Verantwortung für Fehler oder Auslassungen im Inhalt des Dokuments.

In keinem Fall haftet das Unternehmen für besondere, direkte, indirekte oder zufällige Schäden oder für Schäden jeglicher Art, die sich aus der Nutzung des Inhalts des Dokuments ergeben, unabhängig davon, ob es sich um eine Klage aufgrund von Vertrag, Fahrlässigkeit oder anderen Delikten handelt. Das Unternehmen behält sich das Recht vor, den Inhalt des Dokuments jederzeit und ohne vorherige Ankündigung zu ergänzen, zu streichen oder zu ändern.

Haftungsausschluss für Fehler und Auslassungen

Die in dem Dokument enthaltenen Informationen dienen lediglich als allgemeine Orientierungshilfe zu Fragen von Interesse. Daher können Fehler auftreten, auch wenn das Unternehmen alle Vorsichtsmaßnahmen ergreift, um sicherzustellen, dass der Inhalt des Dokuments aktuell und korrekt ist. Außerdem kann es angesichts der sich ändernden Gesetze, Regeln und Vorschriften zu Verzögerungen, Auslassungen oder Ungenauigkeiten bei den in diesem Dokument enthaltenen Informationen kommen.

Das Unternehmen haftet nicht für etwaige Fehler oder Auslassungen oder für die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben.

Haftungsausschluss für faire Nutzung

Das Unternehmen darf urheberrechtlich geschütztes Material verwenden, das der Urheberrechtsinhaber nicht ausdrücklich genehmigt hat. Das Unternehmen stellt dieses Material für Kritik, Kommentare, Berichterstattung, Schulung, Wissenschaft oder Forschung zur Verfügung.

Das Unternehmen ist der Ansicht, dass dies eine „faire Nutzung“ von urheberrechtlich geschütztem Material im Sinne von Abschnitt 107 des US-Urheberrechtsgesetzes darstellt.

Wenn Sie urheberrechtlich geschütztes Material aus dem Dokument für Ihre eigenen Zwecke verwenden möchten, die über eine angemessene Nutzung hinausgehen, müssen Sie die Erlaubnis des Urheberrechtsinhabers einholen.

„Benutzung auf eigene Gefahr“ Haftungsausschluss

Alle Informationen in diesem Dokument werden im Ist-Zustand zur Verfügung gestellt, ohne Garantie auf Vollständigkeit, Genauigkeit, Aktualität oder auf die Ergebnisse, die sich aus der Verwendung dieser Informationen ergeben, und ohne jegliche ausdrückliche oder stillschweigende Garantie, einschließlich, aber nicht beschränkt auf Garantien für Leistung, Marktgängigkeit und Eignung für einen bestimmten Zweck.

Das Unternehmen haftet weder Ihnen noch anderen gegenüber für Entscheidungen oder Handlungen, die im Vertrauen auf die Informationen des Dienstes getroffen wurden, noch für Folgeschäden, besondere oder ähnliche Schäden, selbst wenn auf die Möglichkeit solcher Schäden hingewiesen wurde.

Kontaktieren Sie uns

Wenn Sie Fragen zu diesem Haftungsausschluss haben, können Sie uns per E-Mail kontaktieren: support@vitextra.com.

Inhaltsverzeichnis

Einführung 4

Wichtige Funktionen 5

Funktionsweise 6

- **Wo die Einträge gespeichert werden** 6
- **Verschlüsselung und PIN** 6
- **Arbeiten auf mehreren Geräten** 7

Wofür Password Vault gedacht ist 8

Voraussetzungen 8

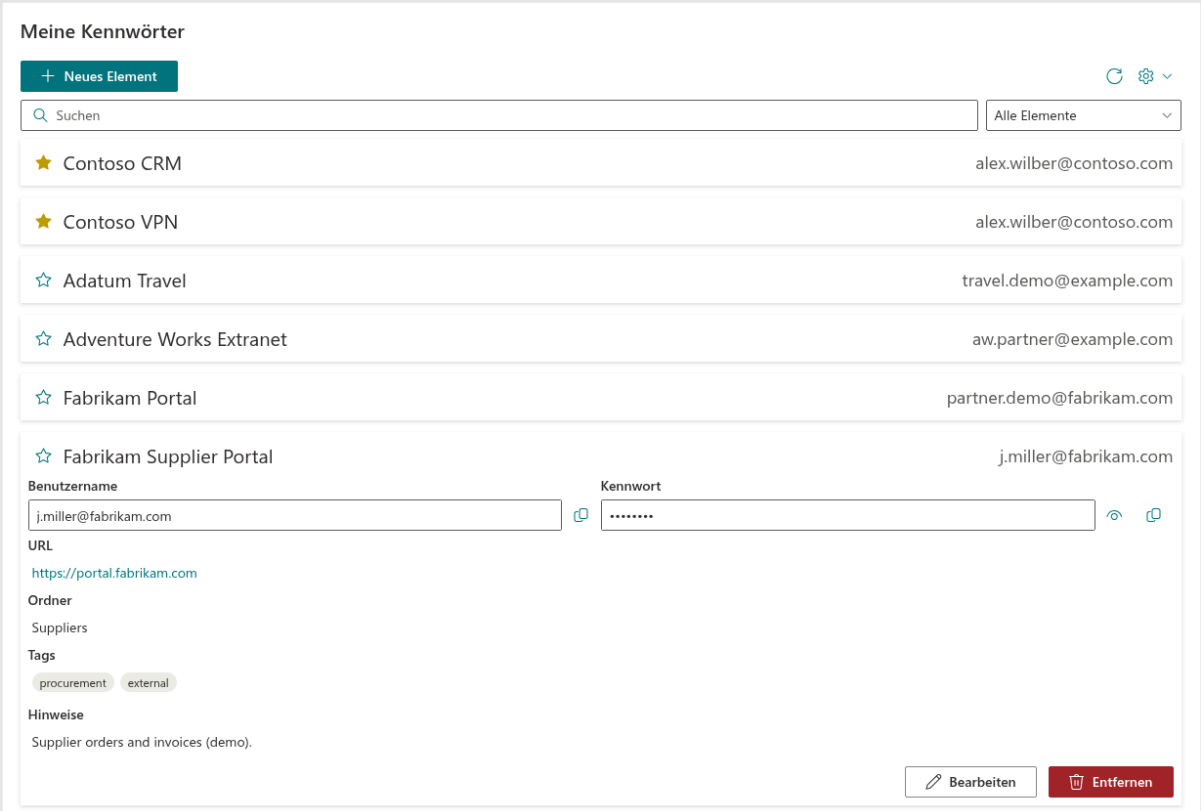
Begriffe 10

Einführung

Mitarbeiter sammeln Anmeldedaten für viele Systeme, die nicht durch einmaliges Anmelden (Single Sign-On) abgedeckt sind: Lieferantenportale, Partner-Extranets, Testumgebungen, Konferenzanmeldungen, Hardwarekonsolen. Ohne ein eigenes Werkzeug landen diese Anmeldedaten in Tabellen, auf Haftnotizen oder in E-Mail-Entwürfen.

Password Vault ist ein SharePoint-Framework-Webpart, das jedem Mitarbeiter einen persönlichen Kennwortmanager in **Microsoft 365** bietet. Jeder Benutzer führt seine eigene **Liste** von Einträgen – Name, Benutzername, Kennwort, URL, Hinweise, Ordner und Tags –, geschützt durch eine 4-stellige PIN. Die Einträge werden verschlüsselt in einer Datei im eigenen OneDrive des Benutzers gespeichert, nicht in SharePoint-Listen und nicht auf Vitextra-Servern. Dasselbe **Webpart** kann auf einer SharePoint-Seite oder in **Microsoft Teams** platziert werden, und jeder Benutzer sieht immer seinen eigenen Tresor.

Dieser Artikel erklärt, was das Webpart tut und wie es funktioniert. Wie Sie es auf einer Seite platzieren, lesen Sie in KB10438. So fügen Sie das Password Vault-Webpart einer Seite hinzu und erstellen Ihren Tresor.



Password Vault auf einer SharePoint-Seite

Wichtige Funktionen

Ein persönlicher Tresor für jeden Benutzer. Das Webpart zeigt den Tresor der Person, die die Seite öffnet. Wenn Sie es auf einer gemeinsam genutzten Seite oder in einem Teamkanal platzieren, werden dadurch keine Kennwörter geteilt: Jeder Besucher sieht nur seine eigenen Einträge.

PIN-Schutz. Bei der ersten Verwendung legt der Benutzer eine 4-stellige PIN fest. Solange der Tresor gesperrt ist, zeigt das Webpart keinen einzigen Eintrag an, sondern nur eine Abfrage der PIN; nach Eingabe der PIN stehen alle Einträge und Aktionen zur Verfügung. Siehe KB10442. So richten Sie Ihre PIN in Password Vault ein.

Automatische Sperre. Nach Eingabe der PIN bleibt der Tresor entsperrt, solange der Benutzer damit arbeitet, und wird nach 5 Minuten ohne Interaktion wieder gesperrt: Die Liste wird ausgeblendet, und geöffnete Dialoge werden geschlossen. Auch das Neuladen der Seite sperrt ihn. Siehe KB10451. Automatische Sperre: Wann Password Vault erneut nach der PIN fragt.

Einträge mit allen Details. Jeder Eintrag hat die Felder **Name**, **Benutzername**, **Kennwort**, ein optionales Feld **URL**, dessen Link in einer neuen Registerkarte geöffnet wird, sowie **Ordner**, **Tags** und **Hinweise**. Siehe KB10443. So fügen Sie Einträge in Password Vault hinzu, bearbeiten und löschen sie.

Kopieren mit einem Klick. Benutzername und Kennwort werden mit den Schaltflächen **In Zwischenablage kopieren** in die Zwischenablage kopiert, sodass Kennwörter nicht auf dem Bildschirm angezeigt werden müssen. Siehe KB10444. So zeigen Sie ein Kennwort oder einen Benutzernamen in Password Vault an und kopieren sie.

Kennwortgenerator. Der integrierte Generator erstellt zufällige Kennwörter mit 8 bis 64 Zeichen aus den Zeichensätzen, die der Benutzer auswählt, und verwendet dafür den kryptografischen Zufallszahlengenerator des Browsers. Siehe KB10445. So generieren Sie ein starkes Kennwort mit dem Kennwortgenerator von Password Vault.

Stärkeanzeige. Während ein Kennwort eingegeben wird, zeigt ein fünfstufiger Balken seine geschätzte Stärke an, von *Sehr schwach* bis *Sehr stark*. Siehe KB10446. Kennwort-Stärkeanzeige in Password Vault: Was die Stufen bedeuten.

Ordner, Tags und Favoriten. Einträge können in Ordnern gruppiert, mit Tags versehen und als Favoriten markiert werden; Favoriten stehen immer oben in der Liste. Siehe KB10447. Einträge mit Ordnern und Tags in Password Vault organisieren und KB10448. Favoriten in Password Vault: Häufig verwendete Einträge oben halten.

Suche und Filter. Das Feld **Suchen** findet Einträge nach Name, Benutzername, URL,

Ordner, Hinweisen und Tags; die Filter-Dropdownliste schränkt die Liste auf Favoriten, einen Ordner oder ein Tag ein. Siehe KB10449. Einträge in Password Vault suchen und filtern.

und Microsoft Teams. Das Webpart funktioniert auf modernen SharePoint Online-Seiten, als Teams-Kanalregisterkarte und als persönliche **Teams-App Passwords**. Überall ist es derselbe Tresor.

Design und Sprache. Das Webpart übernimmt das Design der **Website**, einschließlich Abschnittshintergründen, sowie die Schriftart der Website. Die Benutzeroberfläche ist in die SharePoint-Sprachen übersetzt und folgt der Sprache von SharePoint bzw. Teams. In einer schmalen Spalte (weniger als 500 Pixel breit) wechselt die Liste zu einem kompakten Layout.

Funktionsweise

Wo die Einträge gespeichert werden

Der Tresor jedes Benutzers ist eine einzelne Datei, `vitextra-password-vault.json`, im App-Ordner des eigenen OneDrive dieses Benutzers. Das Webpart liest und schreibt die Datei über **Microsoft Graph** im Namen des angemeldeten Benutzers. Nichts wird in SharePoint-Listen, in den Webpart-Eigenschaften oder auf Vitextra-Servern gespeichert.

Da sich der Tresor im OneDrive des Benutzers befindet und nicht auf der Seite, erscheint derselbe Tresor auf jeder Seite, Website und **Teams-Registerkarte**, auf der das Webpart platziert ist. Findet das Webpart keine Tresordatei für den Benutzer, erstellt es eine leere und fordert den Benutzer auf, eine PIN einzurichten. Details: KB10453. Wo Password Vault Ihre Kennwörter speichert: Der App-Ordner in OneDrive.

Verschlüsselung und PIN

Name, Benutzername, Kennwort, URL, Hinweise, Ordner und Tags jedes Eintrags werden im Browser des Benutzers mit AES verschlüsselt, bevor die Datei gespeichert wird. Der Schlüssel wird mit PBKDF2-SHA256 aus der PIN abgeleitet (ein zufälliger Salt pro Tresor, 600.000 Iterationen); er wird nirgends gespeichert und existiert nur im Arbeitsspeicher der geöffneten Seite, solange der Tresor entsperrt ist. Die Tresordatei allein reicht daher nicht aus, um die Einträge zu lesen. Die Datei wird nur zwischen dem Browser und dem OneDrive des Benutzers übertragen, und der Zugriff darauf wird durch die Berechtigungen von Microsoft 365 und OneDrive geregelt – wie bei jeder anderen Datei im OneDrive des Benutzers.

Die PIN öffnet den Tresor. Solange der Tresor gesperrt ist, zeigt das Webpart keine Einträge an – nicht einmal deren Namen –, sondern nur die Abfrage **PIN eingeben** mit vier Feldern, in denen die Ziffern maskiert sind. Beachten Sie, dass eine PIN nur 4 Ziffern hat (10.000 Kombinationen): PBKDF2 verlangsamt jeden Rateversuch absichtlich, doch wer eine Kopie der Datei erlangt, könnte trotzdem offline alle PINs durchprobieren, denn die Grenze von 5 Versuchen gilt nur innerhalb des Webparts. Die Zugriffssteuerung für OneDrive bleibt deshalb die erste Schutzebene. Die vollständige Beschreibung finden Sie in KB10452. Wie Password Vault Ihre Daten schützt: Verschlüsselung, PIN und Speicherung und KB10456. Wer Ihre Kennwörter in Password Vault sehen kann.

Warnung

Ist der Tresor noch entsperrt, können Sie die PIN ändern, ohne die alte PIN einzugeben. Schließen Sie die Änderung ab und speichern Sie sie, bevor der Tresor gesperrt wird; bei erfolgreichem Speichern bleiben die Einträge erhalten. Sind alle Sitzungen gesperrt und haben Sie die PIN vergessen, bietet Password Vault weder Ihnen noch Ihrem Administrator oder Vitextra eine Wiederherstellungsfunktion. Das Zurücksetzen eines blockierten Tresors löscht alle Einträge. Bewahren Sie wichtige Zugangsdaten zusätzlich an einem anderen von Ihrer Organisation genehmigten Ort auf. KB10455. Falsche PIN-Eingaben in Password Vault: Was nach fünf Fehlversuchen passiert · KB10460. PIN für Password Vault vergessen: Welche Möglichkeiten habe ich?

Hinweis

Tresore, die mit einer früheren Version des Webparts erstellt wurden, werden automatisch auf die neue Verschlüsselung umgestellt, wenn der Benutzer zum ersten Mal die richtige PIN eingibt; die Einträge und ihre Änderungsdaten bleiben erhalten. Ältere Versionen des Webparts können einen umgestellten Tresor nicht öffnen, daher sollten Administratoren Password Vault in jedem **App-Katalog** des Mandanten aktualisieren. Siehe KB10050. So aktualisieren Sie eine Vitextra-SPFx-Lösung in SharePoint Online und KB10361. Mandanten-App-Katalog oder Websitesammlungs-App-Katalog: Wo Vitextra-Apps bereitgestellt werden.

Arbeiten auf mehreren Geräten

Jedes Speichern wird mit der zugrunde liegenden Dateiversion abgeglichen. Hat eine andere Sitzung inzwischen gespeichert, lädt das Webpart die neueste Datei und

wiederholt die Änderung; Änderungen an anderen Einträgen bleiben erhalten. Bearbeiten zwei Sitzungen denselben Eintrag, ersetzt der zuletzt erfolgreich gespeicherte Entwurf den gesamten Eintrag; einzelne Felder werden nicht zusammengeführt. Änderungen von einem anderen Gerät erscheinen nach **Aktualisieren**, dem nächsten Speichern oder Entsperren. Wurde die PIN anderswo geändert, sperrt sich die Seite beim nächsten Lesen der neuesten Datei — beim Aktualisieren, Entsperren oder Speichern — und fragt nach der neuen PIN.

Wofür Password Vault gedacht ist

Password Vault ist ein schlanker **persönlicher** Tresor. Der Funktionsumfang ist bewusst eng gehalten:

- Einträge können nicht mit Kollegen geteilt werden; es gibt keine Team- oder gemeinsamen Tresore.
- Es gibt keine Browsererweiterung und kein automatisches Ausfüllen von Anmeldeformularen; Anmeldedaten werden aus dem Webpart kopiert.
- Administratoren haben keine Konsole, um die Tresore der Benutzer zu verwalten, einzusehen oder wiederherzustellen.
- Es gibt keinen Export und keinen Import von Einträgen.

Einen Vergleich mit anderen Arten von Kennwortmanagern finden Sie in KB10440. Password Vault im Vergleich zu Browser-Kennwortmanagern und Enterprise-Kennwortmanagern: Was ist die richtige Wahl?.

Hinweis

Password Vault ist für persönliche Anmeldedaten gedacht. Für hochprivilegierte Administratorkonten und Anmeldedaten, die ein Team gemeinsam nutzen muss, befolgen Sie die Sicherheitsrichtlinie Ihrer Organisation.

Voraussetzungen

- Microsoft 365 mit **SharePoint Online**; moderne Seiten. Das Webpart ist für SharePoint Server nicht verfügbar.
- Jeder Benutzer muss ein OneDrive im Mandanten haben, da der Tresor dort gespeichert wird.
- Das Paket wird wie jedes Vitextra-Produkt aus dem App-Katalog bereitgestellt; die mandantenweite Bereitstellung wird unterstützt. Siehe KB10035. So installieren Sie ein Vitextra-Produkt in SharePoint Online.
- Ein Administrator muss die delegierte Microsoft-Graph-Berechtigung `Files.ReadWrite.AppFolder` genehmigen, mit der das Webpart nur in seinem

eigenen App-Ordner im OneDrive des Benutzers lesen und schreiben kann. Siehe KB10454. Microsoft-Graph-Berechtigung Files.ReadWrite.AppFolder: Warum Password Vault sie benötigt und wie Sie sie genehmigen und KB10360. So genehmigen Sie Microsoft-Graph-API-Berechtigungen für Vitextra-Lösungen im SharePoint Admin Center.

- Berechtigungen für SharePoint-Listen sind nicht erforderlich: Jeder Benutzer, der die Seite öffnen kann, kann seinen eigenen Tresor verwenden.
- Die Lizenzierung erfolgt pro **Mandant**. Wenn die Lizenz abläuft, zeigt das Webpart anstelle des Tresors *Wir hoffen, Ihre kostenlose Testversion hat Ihnen gefallen. Kaufen Sie sie jetzt, damit Sie weiter damit arbeiten können.* an, bis die Lizenz verlängert wird; die Tresordateien in OneDrive werden nicht verändert. Siehe KB10206. Vitextra Lizenzierung und Konto: Lizenz kaufen und aktivieren und KB10364. Was passiert, wenn Ihre Vitextra-Testversion oder Ihr Abonnement abläuft.

Tipp

Neue Benutzer beginnen am besten mit KB10441. Password Vault: Kurzanleitung für Endbenutzer. Antworten auf häufige Fragen finden Sie in KB10439. Password Vault: Häufig gestellte Fragen.

Weitere Informationen zum Produkt: *https://vitextra.com/de/products/password-vault*

Begriffe

App-Katalog
Der App-Katalog ist eine spezielle SharePoint-Website, in der Apps für SharePoint, Teams und andere Microsoft 365-Dienste gespeichert werden. Globale oder SharePoint-Administratoren können Anwendungen aus dem AppSource-Marktplatz, benutzerdefiniert entwickelte Apps oder Apps von Drittanbietern für die interne Verwendung in der Organisation hochladen und verwalten. In einem Mandanten kann es nur einen App-Katalog auf Mandantenebene geben; für einzelne Websitesammlungen können zusätzliche App-Kataloge für Websitesammlungen hinzugefügt werden.

Liste
Eine Liste ist eine Speichereinheit in SharePoint. Eine Liste kann Spalten unterschiedlicher Typen, Inhaltstypen und Ansichten enthalten. Eine Dokumentbibliothek ist ein spezieller Listentyp und erbt daher die Funktionalität einer Liste.

Mandant
Ein Microsoft 365-Mandant (Tenant) ist eine dedizierte Instanz der Microsoft 365-Dienste. Der Mandant enthält die Informationen der Organisation, z. B. Benutzer und Domänen (Microsoft Entra ID), Konfigurationen, Abonnements und Dienste. Eine Organisation erhält einen Mandanten, indem sie sich für Microsoft 365-Dienste registriert.

Microsoft 365
Microsoft 365 ist ein cloudbasierter Abonnementdienst, der Produktivitäts-Apps wie Word, Excel, PowerPoint und Outlook mit Clouddiensten wie SharePoint, OneDrive, Teams und Exchange Online sowie mit erweiterten Sicherheits- und Geräteverwaltungsfunktionen kombiniert.

Microsoft Graph
Microsoft Graph ist eine REST-API, die mit Microsoft Entra ID (früher Azure Active Directory) und OAuth 2.0 gesichert ist. Sie stellt einen einzigen Endpunkt für den Zugriff auf Daten und Dienste in Microsoft 365 bereit, z. B. SharePoint, Outlook, OneDrive, Teams und weitere.

Microsoft Teams

Begriffe

Microsoft Teams ist eine chatbasierte Zusammenarbeitsplattform für die Unternehmenskommunikation mit Funktionen für Onlinebesprechungen, Liveereignisse und die gemeinsame Nutzung von Dokumenten.

SharePoint Online
Die Cloudversion von SharePoint, einer webbasierten Zusammenarbeitsplattform in Microsoft 365, die umfangreiche Funktionen zum Speichern, Freigeben und Verwalten der digitalen Informationen, Inhalte und des Wissens einer Organisation bietet.

Teams-App
Eine Teams-App ist eine Anwendung, die Microsoft Teams um Funktionen wie Registerkarten, Bots, Nachrichtenerweiterungen und Besprechungserweiterungen ergänzt. Teams-Apps werden als App-Pakete über den Teams-App-Store, AppSource oder den Katalog der Organisation verteilt.

Teams-Registerkarte
Eine Registerkarte in Microsoft Teams ist eine Seite, die in einen Kanal, einen Chat oder eine Besprechung eingebettet ist und Webinhalte oder eine App anzeigt, z. B. eine SharePoint-Seite oder eine benutzerdefinierte Anwendung, am oberen Rand der Unterhaltung.

Webpart
Ein Webpart ist ein grundlegender Baustein für Funktionalität oder Inhalte, der auf einer SharePoint-Seite platziert wird. Einige Webparts unterstützen Anpassungen, z. B. das Konfigurieren des Webparts oder das Ändern seines Erscheinungsbilds.

Website
Eine SharePoint-Website ist ein Container für Informationen innerhalb der SharePoint-Plattform. Websites bieten in der Regel Funktionen wie Dokumentbibliotheken, Listen, Kalender, Diskussionsforen und Workflows und erleichtern so die Zusammenarbeit, Kommunikation und Dokumentverwaltung innerhalb von Teams oder abteilungsübergreifend. Websites können angepasst und konfiguriert werden, um die spezifischen Anforderungen und Workflows einer Organisation zu erfüllen.