

White Paper Dokumentensicherheit

Copyright © 2024 DocuWare GmbH

Alle Rechte vorbehalten

Die Software enthält Proprietary-Information von DocuWare. Sie wird unter Lizenz bereitgestellt und ist darüber hinaus durch das Copyright geschützt. Im Lizenzvertrag sind Einschränkungen bezüglich der Nutzung und Offenlegung enthalten. Rekonstruktion der Software ist untersagt.

Da dieses Produkt laufend weiterentwickelt wird, können die hier enthaltenen Informationen ohne Vorankündigung geändert werden. Die hier enthaltenen Rechte am geistigen Eigentum und Informationen sind vertrauliche Informationen, die nur der DocuWare GmbH und dem Kunden zugänglich sind, und bleiben das ausschließliche Eigentum von DocuWare. Falls Sie in der Dokumentation auf Probleme stoßen, weisen Sie uns bitte in schriftlicher Form darauf hin. DocuWare übernimmt keine Garantie dafür, dass dieses Dokument frei von Fehlern ist.

Kein Teil dieser Veröffentlichung darf ohne die vorherige schriftliche Genehmigung von DocuWare in irgendeiner Form oder mithilfe welcher Verfahren auch immer (elektronisch, mechanisch, Fotokopie, Aufzeichnung oder auf andere Weise) vervielfältigt, in einem Retrievalsystem abgelegt oder übertragen werden.

Dieses Dokument wurde erstellt mit AuthorIT.

Disclaimer

Dieses Dokument wurde mit größter Sorgfalt zusammengestellt und die Informationen darin sind Quellen entnommen, die als zuverlässig gelten. Dennoch kann keine Haftung übernommen werden für die Richtigkeit, Vollständigkeit und Aktualität der Informationen. Aus den in diesem Dokument aufgenommenen Informationen können keine Ansprüche hergeleitet werden. Die DocuWare GmbH behält sich das Recht vor, jegliche Informationen, die in diesem Dokument enthalten sind, ohne vorherige Ankündigung zu verändern.

Gender Hinweis

Bei DocuWare steht jeder einzelne Mensch an oberster Stelle. Das Unternehmen schließt alle Identitäten in der internen sowie externen Kommunikation ein und garantiert damit die Gleichstellung und den Respekt gegenüber allen Individuen. Entsprechend beziehen sich alle vom Unternehmen ehemals sowie zukünftig veröffentlichten Beiträge, auch wenn nicht explizit der Formulierung zu entnehmen, auf alle Geschlechtsidentitäten.

DocuWare GmbH
Planegger Straße 1
82110 Germering
www.docuware.com

Inhalt

1.	Zielsetzung dieses White Papers.	4
2.	Einführung in DocuWare.	5
3.	Zugang zum DocuWare System.	6
3.1	Loginverfahren.	6
3.2	Passwörter.	6
3.3	Kommunikation der Komponenten.	7
4.	Authentizität: Echtheit der Dokumente.	8
4.1	Systemeinträge zu Dokumenten.	8
4.2	Elektronische Signaturen.	8
5.	Vertraulichkeit: Dokumentenzugriff nur für berechtigte Benutzer.	9
5.1	Berechtigungen.	9
5.2	DocuWare als Hochsicherheitssystem.	10
5.3	Dokumente verschlüsseln.	11
6.	Integrität von Daten und Dokumenten.	12
6.1	Änderungen als neue Versionen speichern.	12
6.2	Protokollierung von Benutzer-Ereignissen.	13
7.	Verfügbarkeit des DocuWare Systems.	14
8.	Datensicherung.	15

1 Zielsetzung dieses White Papers

Die Informationssicherheit ist ein wichtiger Faktor für den Erfolg eines Unternehmens. Während jedoch der Schutz von personenbezogenen Daten gesetzlich detailliert geregelt ist, können Unternehmen und Organisationen zur Wahrung der Informationssicherheit unterschiedliche Konzepte einführen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt mit dem IT-Grundschutz-Kompendium einen Leitfaden für Unternehmen und Organisationen zur Sicherung von Informationen und IT-Systemen heraus. In diesem Kompendium werden in Anlehnung an die Anforderungen der ISO 27001 – der internationalen Norm zum Aufbau eines Informationssicherheits-Managementsystems – mit Vertraulichkeit, Integrität und Verfügbarkeit drei Grundwerte, bzw. Schutzziele genannt, die, je nach Risikoeinschätzung eines Unternehmens, erweitert werden können.

In diesem White Paper erfahren Sie, welche Maßnahmen DocuWare als Enterprise Management System für die Umsetzung dieser grundlegenden Sicherheitsziele in Bezug auf die in DocuWare archivierten Dokumente bietet:

- Vertraulichkeit: Dokumente und Daten sind nur für berechtigte Benutzer zugänglich und vor unbefugter Preisgabe von Informationen geschützt.
- Integrität: Dokumente und Daten können nicht unautorisiert geändert werden, Änderungen lassen sich nachvollziehen
- Verfügbarkeit: Dokumente und Dienste von DocuWare stehen jederzeit zur Verfügung
- Zugangs- und Zugriffssicherheit zum DocuWare-System
- Sicherung der in DocuWare gespeicherten Daten

Nicht Thema dieses White Papers sind die Einrichtung eines DocuWare Systems, die Einbettung von DocuWare in die IT-Infrastruktur des Unternehmens, die Sicherung von Datenbanken und des Dateisystems außerhalb von DocuWare, der Schutz der lokalen Rechner sowie DocuWare als Service Provider (DocuWare Cloud).

Ziel des White Papers ist es, Ihnen zu ermöglichen, sich ein technisch fundiertes Urteil über die Sicherheit der in DocuWare gespeicherten Dokumente in einem lokal installierten oder in DocuWare Cloud zu bilden. Sofern Unterschiede zwischen den beiden Systemen bestehen, wird im Einzelnen darauf hingewiesen.

Das White Paper richtet sich an technisch interessierte Leser, vor allem an technische Mitarbeiter bei Kunden, Vertriebspartnern und Beratungsunternehmen, sowie an Fachmedien. Vorausgesetzt wird lediglich ein technisches Grundlagenwissen über den Aufbau moderner Software-Anwendungen, idealerweise von Enterprise Management Systemen.

2 Einführung in DocuWare

DocuWare ist eine Lösung für Dokumentenmanagement und Workflow-Automation. Mit DocuWare greifen Benutzer zu jedem Zeitpunkt und von jedem Ort aus auf ihre Dokumente und die wichtigen Informationen darin zu.

Die Dokumente werden in Archiven zentral abgelegt und indexiert. Über die Workflow-Automation ist es möglich, Dokumente in Geschäftsprozesse zu integrieren. Über die verschiedenen Anwendungsfelder informiert Sie auch die [DocuWare Webseite](#).

DocuWare folgt in seinem Sicherheitskonzept den Prinzipien der europäischen Datenschutz-Grundverordnung (DSGVO), die in Artikel 25 den Schutz personenbezogener Daten durch Technikgestaltung und datenschutzrechtliche Voreinstellungen fordert.

Wenn Sie mehr über die technischen Aspekte von DocuWare erfahren möchten, finden Sie im DocuWare Knowledge Center und auf der DocuWare Webseite weitere Informationen zu folgenden Themen:

- [White Paper DocuWare On-Premises](#)
- [White Paper Integration](#)
- [White Paper Intelligent Indexing](#)
- [White Paper DocuWare Cloud](#)
- [Compliance und Zertifizierungen](#)

3 Zugang zum DocuWare System

Der Zugriff auf DocuWare und die zentralen Archive ist durch ein Loginverfahren sowie durch einen sicheren Datenaustausch der Komponenten untereinander geschützt.

Im Rahmen der Authentifizierung wird die Identität des Benutzers, der sich anmeldet, geprüft und verifiziert. Dies gilt auch für IT-Komponenten oder Anwendungen, die auf DocuWare zugreifen sollen.

- Mehr Informationen zum Aufbau eines lokal installierten DocuWare Systems im [White Paper DocuWare On-Premises](#)
- Mehr Informationen zum Aufbau von DocuWare Cloud im [White Paper DocuWare Cloud](#).

3.1 Loginverfahren

Die Nutzung von DocuWare erfordert zunächst immer eine Anmeldung beim DocuWare Identity Service. Als zentraler Service ist er für alle Organisationen innerhalb von DocuWare für den Login in DocuWare verantwortlich. Der Benutzer muss sich über Namen und Kennwort als berechtigt ausweisen.

Der Identity Service ermöglicht die [Authentifizierung über Single Sign-on \(SSO\)](#). Der Client meldet sich beim externen Provider an, der wiederum ein Token für den DocuWare Identity Service erzeugt. Dieses Token wird im Browser gespeichert, bis es abläuft oder der Browser-Cache geleert wird. Nach Ablauf des Tokens muss sich der Kunde erneut anmelden, um ein neues Token zu erhalten.

Die Kommunikation der Komponenten erfolgt verschlüsselt über HTTPS.

Auch das Erzwingen von Single-Sign-On ist möglich. Die Nutzer haben damit nicht mehr die Möglichkeit, die Anmeldedaten manuell einzugeben. Durch das Erzwingen von SSO innerhalb von DocuWare lässt sich indirekt auch eine Multi Factor Authentifizierung (MFA) erzwingen, sofern MFA beim Identity Provider eingerichtet ist.

3.2 Passwörter

Außer den Passwörtern der DocuWare Benutzer werden auch das Datenbankserver-Passwort und das Passwort für den Mailserver kryptographisch sicher gespeichert, so dass nur die Serverkomponenten diese entschlüsseln können. Damit sind diese Daten sicher, auch wenn bestimmte Benutzer auf die für die Speicherung verwendeten Datenbanken zugreifen können, etwa für Backup-Zwecke.

Technische Umsetzung

Für die Verschlüsselung von Passwörtern wird der Algorithmus PBKDF2 (Password-Based Key Derivation Function 2) eingesetzt. Dabei wird eine Hashfunktion zusammen mit einem Saltwert auf das Passwort angewendet. Durch die Kombination mit einem Zufallswert entsteht auch bei zwei identischen Passwörtern nicht der gleiche Hashwert. Die Funktion wird danach mehrere tausend Male auf das Ergebnis angewendet. Dieses Verfahren

erschwert es Hackern, durch Brute-Force-Attacken aus dem gehashten Wert auf das ursprüngliche Passwort zu schließen.

Passworteinstellungen

In den Organisationseinstellungen der DocuWare Konfiguration lässt sich festlegen, wie komplex Passwörter sein müssen. Sie definieren beispielsweise, ob ein Groß- oder Kleinbuchstabe, eine Ziffer oder ein Sonderzeichen in der Zeichenfolge enthalten sein müssen. Auch lässt sich die minimale Zeichenzahl eines Passworts festlegen, wie lange es gültig bleibt und ab wie vielen falschen Passworteingaben der Zugang gesperrt wird.

Es wird empfohlen, für Passwörter eine Mindestlänge von 14 Zeichen sowie unterschiedliche Zeichensätze festzusetzen. Auch erhöht es die Sicherheit, zufällig generierte Passwörter zu verwenden.

Der Organisationsadministrator kann zudem in der DocuWare Benutzerverwaltung das Passwort-Zeitlimit für bestimmte Benutzer deaktivieren. Dies ist beispielsweise dann nützlich, wenn sich Dienste als Benutzer bei einem Server anmelden müssen.

Hat der Benutzer sein Passwort vergessen, fordert er über den Anmeldedialog des Web Client ein automatisch generiertes Passwort an. Damit ist es möglich, sich im Web Client einzuloggen und ein neues persönliches Passwort einzugeben.

Alternativ dazu setzt der Organisationsadministrator das Passwort zurück. Dies ist für Benutzer mit der Sicherheitsstufe „Hoch“ allerdings nicht möglich, siehe auch Kapitel DocuWare als Hochsicherheitssystem (Seite 10). Benutzer mit hoher Sicherheitsstufe müssen ihre Passwörter selber erneuern.

3.3 Kommunikation der Komponenten

Um einem Angriff von außen und damit dem unautorisierten Abgriff von Daten vorzubeugen ist es wichtig, die Kommunikation per HTTP zwischen den webbasierten Client-Anwendungen und dem Platform Service mit SSL/TLS abzusichern (HTTPS).

In DocuWare Cloud erfolgt dies automatisch.

Kunden von einem lokal installierten DocuWare System müssen im IIS Manager folgende Schritte vollziehen, um die DocuWare-Komponenten für HTTPS (SSL/TLS) zu konfigurieren:

- Zertifikat bzw. Zertifikate einspielen ("Serverzertifikate", Aktion "Importieren")
- Bindung der Website anpassen und über SSL/TLS erreichbar machen
- Ggf. die HTTP - Bindung aus Sicherheitsgründen entfernen (optional)

4 Authentizität: Echtheit der Dokumente

Daten gelten als authentisch, wenn sie jederzeit ihrem Ursprung zugeordnet werden können. In DocuWare lässt sich die Herkunft der gespeicherten Dokumente anhand von unveränderbaren Systemeinträgen sowie elektronischen Signaturen nachweisen.

4.1 Systemeinträge zu Dokumenten

Bei der Ablage eines Dokuments in DocuWare werden automatisch Systemeinträge erstellt, die zu keiner Zeit von Benutzern in DocuWare geändert werden können. Folgende Systemeinträge zu Benutzer, Datum sowie Dokumentänderungen und -zugriffen geben Aufschluss über den Ursprung des Dokuments:

- Abgelegt von
- Abgelegt am
- Letzte Änderung am
- Letzte Änderung von
- Letzte Inhaltsänderung am
- Letzte Inhaltsänderung von
- Letzer Zugriff am
- Letzter Zugriff von
- Dokument-ID

Systemeinträge rufen Sie über das Kontextmenü eines Dokuments in der Ergebnisliste *Indexeinträge ändern > Systemeinträge* ab.

4.2 Elektronische Signaturen

Eine elektronische Signatur erfüllt den gleichen Zweck wie eine eigenhändige Unterschrift bei Papierdokumenten. Sie stellt sicher, dass ein Dokument wirklich vom Urheber stammt. Auch können Änderungen von Dokumenten anhand von Signaturen nachgeprüft und verifiziert werden.

Mit DocuWare lassen sich elektronische Signaturen mit verschiedenen Sicherheitsstufen umsetzen. Ein DocuWare Stempel mit einer Unterschrift auf einem Dokument ist ein Beispiel für eine einfache Signatur. Um die Infrastruktur für das Signieren von digitalen Dokumenten mit den höheren Sicherheitsstufen "fortgeschritten" und "qualifiziert" bereitzustellen, arbeitet DocuWare mit den externen Signatur-Dienstleistern wie Validated ID oder DocuSign zusammen. Beide Dienstleister bieten mehrere Möglichkeiten der Authentifizierung und zahlreiche Funktionen zum Aufbringen von Signaturen, wie unter anderem Mehrfachsignatur oder die biometrische Signatur.

Hier finden Sie

- technische Informationen zu [Signatur-Workflows mit Validated ID und DocuSign](#)
- allgemeine Informationen zu [Sicherheitsstufen von Signaturen](#).

5 Vertraulichkeit: Dokumentenzugriff nur für berechtigte Benutzer

Mitarbeiter und Angestellte sind häufig in zahlreiche Abläufe eingebunden. Um ihre Aufgaben zu erfüllen, benötigen sie Berechtigungen zur Benutzung verschiedener Ressourcen, z.B. Dokumenten- und IT-Funktionen.

Um das Sicherheitsziel "Vertraulichkeit" zu erreichen, sind jedoch auch Beschränkungen erforderlich. Bestimmte Befugnisse sollen nur berechtigten Personen erteilt werden, Dokumente und Daten dürfen nur von autorisierten Benutzern eingesehen beziehungsweise verändert werden.

Folgende Maßnahmen in DocuWare ermöglichen die Umsetzung solcher komplexen Szenarien:

- Steuern Sie den Dokumentenzugriff über Berechtigungen (Seite 9).
- DocuWare als Hochsicherheitssystem (Seite 10) bietet zusätzliche Sicherheit durch Einschränkungen bei der Berechtigungsvergabe. Mit DocuWare als Hochsicherheitssystem verhindern Sie, dass aus Versehen auf besonders sensible Bereiche in DocuWare zugegriffen werden kann – zum Beispiel über fehlerhafte Gruppen und Rollenzuweisungen.
- Sensible Dokumente sind dank der standardmäßigen 256 Bit-Verschlüsselungen (Seite 11) auch auf Administrator-Ebene vor unberechtigtem Zugriff geschützt.

Kunden von lokal installierten DocuWare Systemen (On-Premises) beachten bitte:

Bestimmte für DocuWare relevante Daten lassen sich nicht mit DocuWare Berechtigungen oder anderen Sicherheitsmaßnahmen schützen. Dazu gehören die Indexdaten zu den Dokumenten und der extrahierte Volltext, die in den jeweiligen Datenbanken abgelegt werden.

Wie Sie diese Informationen schützen, entnehmen Sie bitte dem White Paper DocuWare On-Premises – Systemarchitektur im Kapitel Sicherheit und externer Zugriff.

5.1 Berechtigungen

Das Rechtekonzept von DocuWare unterscheidet zwischen funktionalen Rechten, Archivrechten und Objektrechten, mit denen Sie den Handlungsspielraum jeden Benutzers präzise steuern.

- Funktionale Rechte sind Rechte auf bestimmte Programmfunktionalitäten. Dazu gehört zum Beispiel das Recht, einen Stempel oder einen Briefkorb anzulegen.
- Archivrechte sind auf ein Archiv und die darin gespeicherten Dokumente bezogen, wie das Ablegen und Suchen eines Dokuments, die Änderungen von Indexeinträgen oder den Export von Dokumenten oder eines Archivs in das Dateiverzeichnis. Für verschiedene Archive können verschiedene Archivrechte vergeben werden.
- Objektrechte: Einige Objekte wie Briefkörbe, Archive oder Formulare können den Benutzern als Administrator oder Benutzer zugeordnet werden. Mit dem Benutzerrecht lässt sich das Objekt verwenden, das Administratorrecht enthält das Recht, das Objekt beziehungsweise die zugehörige Konfiguration zu ändern.

Die verschiedenen Berechtigungen werden zu Profilen zusammengefasst und einzelnen oder Gruppen von Mitarbeitern zugewiesen.

Mehr dazu, wie Sie den Handlungsspielraum und den Dokumentenzugriff mit Berechtigungen steuern können, lesen Sie im Grundlagen-Artikel [Berechtigungskonzept](#).

5.2 DocuWare als Hochsicherheitssystem

Um DocuWare On-Premises als Hochsicherheitssystem nutzen zu können, muss einmal die Sicherheitsstufe *Hoch* für das gesamte DocuWare System aktiviert werden (*DocuWare Administration > System*). Wenn Sie DocuWare Cloud nutzen, ist die Sicherheitsstufe *Hoch* standardmäßig aktiviert.

In DocuWare Cloud und in DocuWare On-Premises mit aktivierter Hochsicherheitsstufe kann der Organisationsadministrator die Eigenschaft *Hochsicherheit* bestimmten Benutzern (*DocuWare Konfiguration > Benutzerverwaltung*) und Archiven (*DocuWare Konfiguration > Archive*) zuteilen.

Nur ein Benutzer mit Sicherheitsstufe *Hoch* ist befugt, auf ein Hochsicherheits-Archiv zugreifen.

Folgende weitere Unterschiede gibt es zu einem System ohne die Eigenschaft *Hochsicherheit*:

- Es ist nicht möglich, die Archivprofile für ein Hochsicherheits-Archiv einer Rolle zuzuweisen. Die Archivprofile für ein Hochsicherheits-Archiv müssen Benutzern direkt zugewiesen werden und diese Benutzer ebenfalls über die Eigenschaft *Hochsicherheit* verfügen.
Somit ist ausgeschlossen, dass für besonders sensible Bereiche ein Zugriff ungewollt über Gruppen- und Rollenzuweisungen erfolgen kann.
- Wenn die Eigenschaft *Hochsicherheit* einem Benutzer zugewiesen ist, kann das Benutzerkennwort nur von diesem Benutzer geändert werden. Der Organisationsadministrator kann das Kennwort für diesen Benutzer nur zurücksetzen, aber nicht ändern.
- Für Benutzer mit Sicherheitsstufe *Hoch* ist es nicht möglich, sich über ein Trusted Login anzumelden, da beim Trusted Login die Sicherheit nicht über DocuWare gewährleistet wird.

5.3 Dokumente verschlüsseln

Um sicherzustellen, dass selbst Administratoren nicht unautorisiert sensible Dokumente lesen können, lassen sich in DocuWare Dokumente verschlüsselt speichern. Mit dieser Option können Sie den Zugriff auf Dokumente auch im Dateisystem zuverlässig unterbinden.

Der Schlüssel ist standardmäßig 256 Bit lang.

Beachten Sie bitte speziell für DocuWare On-Premises:

- DWX-Dateien sind nicht verschlüsselt. In DWX-Dateien lassen sich Metadaten zum Dokument zusätzlich zu der Speicherung am Archiv-Speicherort sichern.
- Verschlüsselte Ablagen sind für autorisierte Nutzer nur bei Verfügbarkeit des entsprechenden Schlüssels nutzbar. Die Dokument-Schlüssel werden über ein asymmetrisches Verfahren mit einem in der Datenbank gespeicherten Schlüssel entschlüsselt. Da die Dokumente ohne den Schlüssel in der Datenbank nicht entschlüsselt werden können, muss bei verschlüsselter Ablage darauf geachtet werden, dass von den DocuWare-System-Tabellen ein regelmäßiges Backup erstellt wird, um bei Verlust der Datenbank insbesondere die Schlüssel-Tabellen wieder herstellen zu können.
- Volltext-Dateien können nicht durch DocuWare verschlüsselt werden. Die Indexdaten in der Datenbank sind ebenfalls nicht verschlüsselt. Enthalten diese Daten sensible Informationen, ist auf die Sicherungsmöglichkeiten des Datenbank-Anbieters zurückzugreifen.

6 Integrität von Daten und Dokumenten

Das Sicherheitsziel "Integrität" besagt, dass Daten und Dokumente nicht unautorisiert geändert werden dürfen. Alle Änderungen an einem Dokument müssen nachvollziehbar sein.

DocuWare gewährleistet die Integrität der archivierten Dokumente mit folgenden Maßnahmen (gilt für DocuWare Cloud und DocuWare On-Premises):

- Es ist über das Berechtigungssystem möglich, Dokumente für Benutzer generell zu sperren, beziehungsweise nur für autorisierte Benutzer zugänglich zu machen.

Auch können Sie den Zugriff auf Dokumente generell zulassen, aber einschränken. Dies ist möglich, indem Sie beispielsweise den Benutzern das Leserecht, aber nicht das Bearbeiten-Recht an Dokumenten zuteilen. Mehr dazu lesen Sie im Artikel Das Berechtigungskonzept von DocuWare.

- Mit der Archivfunktion Automatisches Versionsmanagement (Seite 12) lässt sich jederzeit nachvollziehen, ob ein Dokument geändert wurde.
- Die Integrität von archivierten Dokumenten wird mit Hashwerten überprüft. Im Web Client können Sie anhand einer Prüfsumme feststellen, ob ein Dokument auf Dateiebene geändert wurde. Auch Dokumente, die in Briefkästen oder im Archiv mit einem Signaturstempel signiert worden sind, lassen sich mit Hashwerten überprüfen. Für die Prüfsumme wird der Algorithmus Sha-256 eingesetzt.
- DocuWare kann alle benutzerbezogenen Vorgänge innerhalb von DocuWares transparent protokollieren (Seite 13).

6.1 Änderungen als neue Versionen speichern

Wenn für ein Archiv die Funktion *Neue Versionen automatisch erstellen* aktiviert ist, wird ein Dokument, sobald es geändert wird, als neue Version im gleichen Archiv gespeichert. Das heißt, jede Änderung führt automatisch zu einer neuen Dokumentversion.

Bei aktiviertem Versionsmanagement befinden sich in einem Archiv also neben der aktuellen auch ältere Versionen. Ältere Versionen können in der Versionshistorie betrachtet werden. Angezeigt werden unter anderem die Versionsnummern, Status, Speicherdatum, Kommentare sowie der Nutzer, der das Dokument gespeichert hat.

Das in Bearbeitung befindliche Dokument wird aus DocuWare ausgecheckt und gesperrt. Andere Benutzer können das Dokument zwar ansehen, aber nicht selber bearbeiten, bis das Dokument als neue Version wieder eingchecked ist. Es kann jeweils nur die aktuelle Version bearbeitet werden.

Es ist auch möglich, das Versionsmanagement so einzurichten, dass einzelne Dokumente manuell ausgecheckt und als neue Version gespeichert werden. Dann ist natürlich nicht die Integrität für alle Dokumente eines Archivs gewährleistet.

Mehr Informationen zum Thema Versionsmanagement

6.2 Protokollierung von Benutzer-Ereignissen

DocuWare verfügt über eine transparente Protokollierung aller Benutzer-Ereignisse. Mit dem entsprechenden Funktionsrecht sehen Sie auf Dokument-, Archiv-, Organisations- oder Systemebene, wer wann welche Einstellungen geändert oder Dokumente abgelegt hat.

Alle Protokollierungen können Sie in der DocuWare Konfiguration im universellen CSV-Format herunterladen und für Auswertungen in vielen Programmen verwenden.

Beispiele für Ereignisse, die auf den einzelnen Ebenen protokolliert werden, jeweils mit Datum, Zeit und Benutzer:

Dokument: Ablage, Indexänderung mit altem und neuem Wert, Anzeige, Druck, Anfügen von Anmerkungen etc

Archiv: Neue Indexfelder, Änderungen bei Such- und Ablagedialogen sowie Ergebnislisten, neue Archivprofile etc. Zudem alle Dokumentereignisse innerhalb des Archivs.

Organisation: Neue Konfigurationen sowie alle Änderungen an Bestehenden, An- und Abmeldung der Benutzer

System: Änderung an Zeitplänen für automatische Prozesse wie Transfer, Löschregeln, Synchronisation

7 Verfügbarkeit des DocuWare Systems

Um die Geschäftskontinuität zu gewährleisten, sollen ein DocuWare System und seine Services durchgängig betriebsbereit sein. Benutzer können jederzeit auf Dokumente, Daten und Anwendung zugreifen.

- Für DocuWare Cloud ist die Verfügbarkeit der Dienste durch DocuWare als Anbieter sichergestellt – mehr dazu finden Sie im [White Paper DocuWare Cloud](#).
- DocuWare als lokal installiertes Dokumentenmanagement-System ist meist in eine heterogene IT-Infrastruktur eingebettet. Deshalb kann es aus Gründen, die zunächst nichts mit dem DMS zu tun haben, dennoch zu einem Ausfall kommen – beispielsweise durch einen Hardwarecrash oder durch eine Infizierung von Client-Rechnern im Unternehmen mit Schadsoftware. Beidem kann DocuWare durch seine spezielle Architektur vorbeugen. Server und andere Komponenten können mehrfach installiert werden, so dass redundante Komponenten die im Falle eines Hardwarecrashes ausgefallenen Funktionen nahtlos übernehmen können. Mehr dazu finden Sie im White Paper DocuWare On-Premises im Kapitel [Verfügbarkeit und Datensicherung](#).

8 Datensicherung

Für die Daten und Dokumente im DocuWare System sollten Sicherungsläufe etabliert sein, damit sich die Daten im Falle eines Hardwarecrashs unverzüglich wieder einspielen lassen.

- Für DocuWare Cloud ist das Backup und die Verfügbarkeit der Daten durch DocuWare als Anbieter sichergestellt – mehr dazu finden Sie im [White Paper DocuWare Cloud](#).
- Bei lokal installierten DocuWare Systemen ist die Sicherung der DocuWare Datenbanken und Speichorte in der Verantwortung der Unternehmens-IT. Es gibt keinen DocuWare Mechanismus, der die Datenbanken und Speicherorte automatisch sichert.

Welche DocuWare Komponenten für ein Backup im Detail extern gesichert werden sollten, lesen Sie im White Paper DocuWare On-Premises im [Kapitel Verfügbarkeit und Datensicherung](#).