Password Safe und das IT-Grundschutz-Kompendium 2021

MATESO
PASSWORD SAFE

Whitepaper

Einführung

Die Digitalisierung schreitet auch in Deutschland in großen Schritten voran und konfrontiert Unternehmen immer wieder mit neuen Aufgaben, Herausforderungen und Chancen. Die wichtigste Frage ist dabei stets: Wie können Unternehmen ihre Systeme und Daten vor Angriffen von außen schützen? Dafür stellt das Bundesamt für Sicherheit in der Informationstechnik regelmäßig das IT-Grundschutz-Kompendium bereit. Es beinhaltet detaillierte Methoden, Handlungsanweisungen und Empfehlungen, um unternehmenseigene IT-Systeme, Daten und Prozesse bestmöglich zu schützen.

Auch Password Safe trägt dazu bei, die Sicherheit von Unternehmen zu erhöhen und den Zugriff auf Informationen in unserer digitalen Welt sicherer zu machen. Lesen Sie in diesem Whitepaper, wie Sie die Passwort-Empfehlungen des IT-Grundschutzes mit Password Safe bestmöglich umsetzen und Ihr Unternehmen ideal absichern.

Bundesamt für Sicherheit in der Informationstechnik

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden.

Die wichtigsten Features im Überblick

Password Safe bietet zahlreiche Features, um den Umgang mit Passwörtern und anderen Informationen so sicher wie möglich zu gestalten und die Empfehlungen des IT-Grundschutzes umzusetzen.

Rollenbasiertes Rechtesystem	Jeder Mitarbeiter erhält die für seine Rolle notwendigen Zugriffsrechte automatisiert.
Temporäre Freigabe	Passwörter können temporär freigegeben und anschließend wieder entzogen werden.
Sichtschutz	Passwörter können mit einem Sichtschutz hinterlegt werden, sodass Mitarbeiter sie zwar nutzen, aber nicht einsehen können. So bleiben auch geteilte Passwörter geheim.
2-Faktor-Authentifizierung	Mittels einem Token, einer Smartcard oder einem biometrischen Scanner ermöglicht Password Safe die besonders sichere 2-Faktor-Authentifizierung.
Identity Provider	Password Safe kann die Credentials bereitstellen, um sich bei anderen Anwendungen unkompliziert anzumelden.
Passwortlose Anmeldung	Der Nutzer kann sich mit einem Token oder einer Smartcard passwortlos bei Password Safe und von dort aus bei anderen Anwendungen anmelden.
Passwort-Generator	Password Safe verfügt über einen integrierten Passwort-Generator, der hochsichere und komplexe Passwörter entsprechend individueller Richtlinien erstellen kann.
App & Browser-Erweiterung	Für die sichere Anmeldung auch unterwegs bietet Password Safe eine eigene App und eine Browser-Erweiterung.
Password Reset	Passwörter können mit dem Password Reset individuell, aktionsbezogen oder in regelmäßigen Abständen ausgetauscht werden, ohne dass dem Nutzer daraus Nachteile entstehen.
Ende-zu-Ende-Verschlüsselung	Password Safe nutzt die modernsten Verschlüsselungstechnologien und Algorithmen: • AES 256 • PBKDF2 mit 100.000 Iterationen für die Bildung von Benutzer-Hashes • PBKDF2 mit 1.000 Iterationen für die Hashes der Passwörter innerhalb der Datenbank • RSA 4096 für Private- und Public-Key-Verfahren
Siegel & Mehr-Augen-Prinzip	Durch ein Siegel kann ein Passwort erst genutzt oder eingesehen werden, wenn das Siegel durch einen oder mehrere Berechtigte gebrochen wurde.
Notfall-Absicherung	Für Notfälle steht ein OfflineClient für Windows, ein WebViewer für den Browser sowie ein 2FA-geschützter Notfall WebViewer für Administratoren zur Verfügung.

Passwortspezifische IT-Grundschutz-Empfehlungen im Detail

ORP.4: Identitäts- und Berechtigungsmanagement

2.1 Fehlende oder unzureichende Prozesse beim Identitäts- und Berechtigungsmanagement

„Sind Prozesse beim Identitäts- und Berechtigungsmanagement unzureichend definiert oder implementiert, ist nicht gewährleistet, dass Zugriffe auf das erforderliche Maß eingeschränkt sind und so gegen die Prinzipien Need-to-Know bzw. Least-Privilege verstoßen wird. Der Administrator erhält möglicherweise keine Informationen über personelle Veränderungen, sodass beispielsweise eine Benutzerkennung eines ausgeschiedenen Mitarbeiters nicht gelöscht wird. Dieser kann somit weiterhin auf schützenswerte Informationen zugreifen."

Password Safe verfügt über ein **rollenbasiertes Rechtesystem**. So erhalten alle Mitarbeiter die ihrer Rolle entsprechenden Berechtigungen für in Password Safe hinterlegte Zugangsdaten. HR-Mitarbeiter oder Abteilungsleiter können dazu autorisiert werden, Rollen und die damit verbundenen Zugänge zuzuteilen und zu entziehen. So wird die IT entlastet, Verantwortlichkeiten besser verteilt und Benutzer erhalten mehr Handlungsspielraum, um selbst aktiv zu handeln und Zugangsdaten zu schützen.

„Auch ist es möglich, dass Mitarbeiter, die in eine neue Abteilung versetzt wurden, ihre alten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamtberechtigungen ansammeln."

Dank der **rollenbasierten Rechtevergabe** in Password Safe können Rechte innerhalb einer Abteilung einfach gewährt und auch wieder entzogen werden. **Temporäre Freigaben** erlauben zeitlich begrenzten Mitarbeitern wie Werkstudenten, Auszubildenden oder externen Dienstleistern nur einen eingeschränkten Zugriff auf Zugangsdaten.

Werden die notwendigen Passwörter mit einem **Sichtschutz** belegt, können Mitarbeiter diese zum Login verwenden, aber nicht im Klartext einsehen. So wird gewährleistet, dass etwa Auszubildende auch beim Durchlaufen mehrerer Abteilungen immer nur die aktuell notwendigen Berechtigungen erhalten.

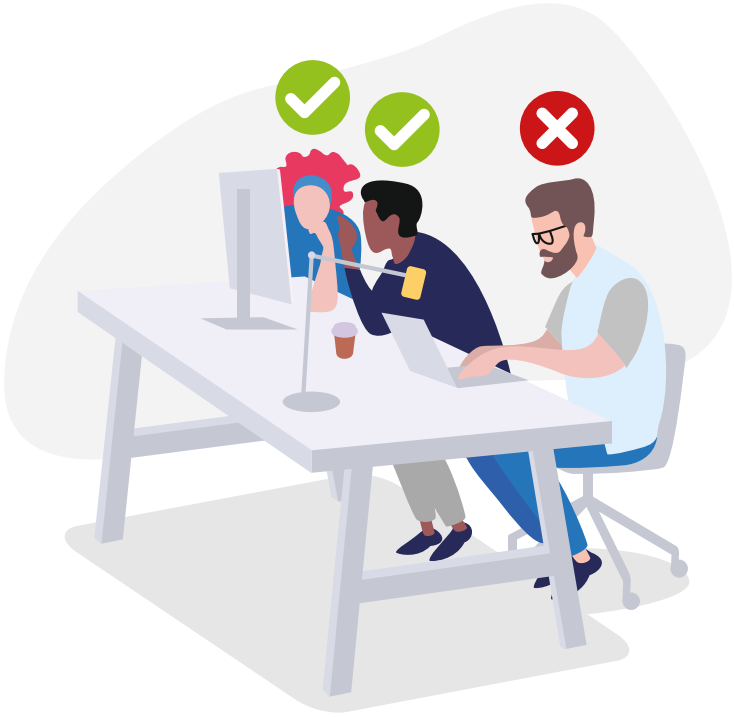
2.2 Fehlende zentrale Deaktivierungsmöglichkeit von Benutzerzugängen

„In Institutionen haben Mitarbeiter oft Benutzerzugänge zu diversen IT-Systemen, wie Produktiv-, Test-, Qualitätssicherungs- oder Projekt-Systeme. Diese befinden sich meist in unterschiedlichen Zuständigkeitsbereichen und werden oft von unterschiedlichen Administratoren verwaltet. Das führt unter Umständen dazu, dass nicht auf allen IT-Systemen eine gleiche und eindeutige Benutzerkennung verwendet wird und es auch keine zentrale Übersicht über die Benutzerzugänge auf den einzelnen IT-Systemen gibt."

In Password Safe können alle Zugangsdaten zentral gespeichert und übersichtlich verwaltet werden. Zudem können Administratoren im Rahmen der Benutzerverwaltung alle User einsehen. So erhalten sie eine zentrale Übersicht über die Benutzer und deren Berechtigungen für einzelne Zugangsdaten.

„In einem solchen Szenario ist es nicht möglich, bei einem Angriff oder einem Passwortdiebstahl in einem Arbeitsschritt alle Benutzerzugänge eines Mitarbeiters zu deaktivieren. Auch können in diesem Szenario bei dem Ausscheiden eines Mitarbeiters aus der Institution nicht in einem Arbeitsschritt alle Zugänge gesperrt werden."

Durch die **rollenbasierte Rechtevergabe** werden Benutzerzugänge nicht abhängig von der Person, sondern abhängig von deren Rolle verwaltet. Diese Rolle und die damit einhergehenden Zugänge können im Rahmen des Rechtemanagements jederzeit von bevollmächtigten Personen entzogen werden. Durch den **Sichtschutz** lässt sich zusätzlich schon im Vorfeld verhindern, dass Mitarbeiter unerlaubt Passwörter einsehen. Im Ernstfall können eventuell kompromittierte Passwörter durch den **Password Reset** automatisiert oder manuell ausgetauscht werden.



ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb]

„Die Institution MUSS den Passwortgebrauch verbindlich regeln (...)."

In Password Safe wird der Gebrauch von Passwörtern inklusive aller hierfür notwendiger Aktionen (Erstellen, Speichern, Teilen, Anmelden, Archivieren) verbindlich geregelt.

„Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können."

Mit der **2-Faktor-Authentifizierung** bietet Password Safe die Möglichkeit, für die hinterlegten Anwendungen zusätzlich zum Passwort mindestens einen weiteren Faktor vorzugeben, beispielsweise durch einen biometrischen Scanner oder einen Token. Außerdem ermöglicht Password Safe als **Identity Provider** auch die **passwortlose Anmeldung** an Anwendungen. Der Login für Password Safe selbst kann passwortlos oder durch die Kombination eines Masterpassworts mit einem FIDO-2-konformen Token oder einer Smartcard erfolgen.

„Passwörter DÜRFEN NICHT mehrfach verwendet werden. Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden."

Durch den in Password Safe integrierten **Passwort-Generator** kann für jede Anwendung ein eigenes komplexes Passwort erstellt und hinterlegt werden. Zudem muss sich der Anwender diese Passwörter nicht merken, da sie sicher in Password Safe gespeichert und abrufbar sind.

„Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden."

Der **Passwort-Generator** schließt leicht zu erratende sowie im Wörterbuch zu findende Wörter systematisch aus. Außerdem lassen sich individuelle Richtlinien anlegen, um die gewünschte Komplexität von Passwörtern zu gewährleisten. Password Safe kann außerdem die Sicherheit von selbsterstellten Passwörtern bewerten.

„Passwörter MÜSSEN geheim gehalten werden. Sie DÜRFEN NUR dem Benutzer persönlich bekannt sein."

In Password Safe werden alle Passwörter sicher und nur für den Berechtigten einsehbar gespeichert. Durch die zusätzliche **Sichtschutz**-Option kann das Passwort nicht im Klartext eingesehen, aber trotzdem zum Login verwendet oder sicher geteilt werden, ohne es zu kennen.

„Passwörter DÜRFEN NUR unbeobachtet eingegeben werden.“

Mithilfe von Password Safe erfolgt der Login automatisch: Ein Eintippen des Passworts ist nicht mehr notwendig, da die Zugangsdaten verdeckt zur Anmeldung weitergegeben werden. So ist eine unbeobachtete Eingabe stets gewährleistet.

Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden.

Der unkomplizierte Login via Password Safe macht es überflüssig, zu solchen unsicheren Behelfslösungen zu greifen. Alle Zugangsdaten werden zentral und sicher gespeichert.

„Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden.“

Mit Password Safe gehört die schriftliche Fixierung von Passwörtern der Vergangenheit an – im Ernstfall kann der **Notfall Web-Viewer** genutzt werden, der die Passwörter in einer verschlüsselten HTML-Datei zur Verfügung stellt.

„Die Nutzung eines Passwort-Managers SOLLTE geprüft werden.“

Ein Password Manager ist heutzutage Teil jeder umfassenden ISMS-Strategie und für Unternehmen, die ihre Passwörter und Geheimnisse schützen wollen, nicht mehr wegzudenken. Password Safe ist der Marktführer für Password Management im DACH-Raum:

20 der 30
DAX-Unternehmen

über 10.000
Firmenkunden
vertrauen auf uns.

„Bei Passwort-Managern mit Funktionen oder Plug-ins, mit denen Passwörter über Onlinedienste Dritter synchronisiert oder anderweitig an Dritte übertragen werden, MÜSSEN diese Funktionen und Plug-ins deaktiviert werden.“

Password Safe überträgt keine Passwörter über Drittsysteme und bietet eine eigene sichere **App** sowie eine eigene **Browser-Erweiterung**.

„Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.“

Der **Password Reset**, um ein Passwort auszutauschen, kann in Password Safe manuell, zeit- oder ereignisbasiert erfolgen. Da Unternehmen oft nicht wissen, wann unautorisierte Personen Zugriff auf ein Passwort hatten, empfiehlt sich ein regelmäßiger, automatisierter Wechsel der Passwörter, um potenzielle Angreifer bewusst auszuschließen. Dank Password Safe entsteht für den Anwender daraus kein zusätzlicher Aufwand und alle Änderungen sind revisionssicher protokolliert.

ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb]

„In Abhängigkeit von Einsatzzweck und Schutzbedarf MÜSSEN sichere Passwörter geeigneter Qualität gewählt werden."

Der in Password Safe integrierte **Passwort-Generator** kann phonetische, benutzerdefinierte oder Richtlinien-basierte Passwörter erstellen. Je nach Einsatzzweck und Schutzbedarf können höhere Passwort-Anforderungen hinterlegt werden.

„Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist. Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden."

Mithilfe von Password Safe muss sich der Benutzer keine Passwörter mehr merken und kann daher hochsichere und komplexe Passwörter verwenden. Die Komplexität der Passwörter ist in den Voreinstellungen in Bezug auf Mindestlänge, Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen und leicht verwechselbare Zeichen definierbar. "Lesbare" Passwörter können als "Phonetisches Passwort" ausgegeben werden.

ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb]

„IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden."

Wo Password Safe im Einsatz ist, bietet ein sicherer zeitgesteuerter Wechsel der Passwörter keine Nachteile. Der Endanwender wird vom manuellen **Password Reset** befreit und muss sich auch keine Passwörter merken. So kann die Sicherheit im Unternehmen erhöht werden.

„Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt und vordefinierte Kennungen MÜSSEN geändert werden.“

Password Safe erkennt neue sowie unsichere Passwörter, die nicht den internen Richtlinien entsprechen, und hinterlegt mithilfe des **Passwort-Generators** einen sicheren Wert.

„Es SOLLTE sichergestellt werden, dass die mögliche Passwortlänge auch im vollen Umfang von verarbeitenden IT-Systemen geprüft wird.“

Password Safe bewertet die Qualität der hinterlegten Passwörter. Außerdem können in Password Safe Mindestanforderungen an die Passwortlänge angelegt werden, um Passwörter, die diese Kriterien unterschreiten, auszuschließen.

„Nach einem Passwortwechsel DÜRFEN alte Passwörter NICHT mehr genutzt werden.“

Password Safe kann alte, unsichere Passwörter mithilfe des **Passwort-Generators** durch neue, automatisch erstellte Passwörter ersetzen. Aufgrund der Komplexität der vom Generator erstellten Werte ist es quasi ausgeschlossen, dass ein altes Passwort mehrfach verwendet wird.

„Passwörter MÜSSEN so sicher wie möglich gespeichert werden.“

Password Safe bietet dank moderner **Ende-zu-Ende-Verschlüsslung** den höchstmöglichen Schutz.

„Bei Kennungen für technische Benutzer, Dienstkonten, Schnittstellen oder Vergleichbares SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.“

Mithilfe von Password Safe verläuft der Wechsel von Passwörtern unkompliziert und für den Nutzer entsteht daraus kein zusätzlicher Aufwand. Eine langfristige Planung für **Password Resets** ist daher nicht notwendig. Dennoch kann der Passwort-Wechsel auch individuell eingestellt und abgestimmt werden.

„Bei der Authentisierung in vernetzten Systemen DÜRFEN Passwörter NICHT unverschlüsselt über unsichere Netze übertragen werden. Wenn Passwörter in einem Intranet übertragen werden, SOLLTEN sie verschlüsselt werden.“

Password Safe bietet eine moderne **Ende-zu-Ende-Verschlüsselung** und erfüllt damit höchste Sicherheitsanforderungen.

„Bei erfolglosen Anmeldeversuchen SOLLTE das System keinen Hinweis darauf geben, ob Passwort oder Benutzerkennung falsch sind.“

Ist die Anmeldung an Password Safe selbst erfolglos, wird kein Hinweis auf falsch eingetragene Zugangsdaten gegeben.

ORP.4.A11 Zurücksetzen von Passwörtern [IT-Betrieb]

„Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Die Support-Mitarbeiter, die Passwörter zurücksetzen können, SOLLTEN entsprechend geschult werden. Bei höherem Schutzbedarf des Passwortes SOLLTE eine Strategie definiert werden, falls ein Support-Mitarbeiter aufgrund fehlender sicherer Möglichkeiten der Übermittlung des Passwortes die Verantwortung nicht übernehmen kann.“

Der **Password Reset** ermöglicht in Password Safe das Zurücksetzen von Passwörtern auf einen neuen und unbekannten Wert gemäß frei definierbarer Auslöser. Ein solcher Auslöser kann sowohl ein definierbares Intervall sein oder eine bestimmte Aktion des Benutzers, wie der Login oder das Ändern des Passwortes. Zum Zurücksetzen von Passwörtern werden entsprechende Rechte benötigt. Der **Password Reset** wird als Aktion im Logbuch dokumentiert und kann so nachvollzogen werden.

ORP.4.A24 Vier-Augen-Prinzip für administrative Tätigkeiten [IT-Betrieb]

„Administrative Tätigkeiten SOLLTEN nur durch zwei Personen durchgeführt werden können. Dazu SOLLTEN bei Mehr-Faktor-Authentisierung die Faktoren auf die zwei Personen verteilt werden. Bei der Nutzung von Passwörtern SOLLTEN diese in zwei Teile zerlegt werden und jede der zwei Personen enthält einen Teil.“

Password Safe bietet das **Mehr-Augen-Prinzip** durch die **Siegel**-Funktion: Das Aufdecken eines Passworts muss erst bei den hinterlegten Personen angefragt und freigegeben werden. Zudem kann vom Nutzer ein Grund für die Anfrage gefordert werden, der in der Historie protokolliert wird. Besonders sicherheitskritische Aktionen werden durch Live-Benachrichtigungen an die zuständigen Personen abgesichert.

CON.8.A5 Sicheres Systemdesign

„Falls zur Authentifizierung Passwörter gespeichert werden, MÜSSEN diese mit einem sicheren Hashverfahren gespeichert werden.“

Password Safe bietet PBKDF2 als Hashverfahren mit 1.000 Integrationen und 100.000 für den Hash des Benutzerpassworts.

OPS.1.1.2.A2 Vertretungsregelungen und Notfallvorsorge

„Es MUSS sichergestellt sein, dass benannte Vertreter auf die zu betreuenden IT-Systeme zugreifen können. Für Notfälle SOLLTEN Notfalluser mit Administrationsrechten eingerichtet werden.“

Mithilfe der **rollenbasierten Rechtevergabe** können Mitarbeiter im Notfall unkompliziert berechtigt werden, Zugriff auf IT-Systeme zu erhalten. Für Notfälle steht ein **Offline-Client** für Windows, ein **WebViewer** für den Browser sowie ein 2FA-geschützter **Notfall WebViewer** für Administratoren zur Verfügung.

OPS.1.1.2.A4 Beendigung der Tätigkeit als IT-Administrator [Personalabteilung]

„Wenn Administratoren von ihren Aufgaben wieder entbunden werden, MÜSSEN alle ihnen zugewiesenen persönlichen Administrationskennungen gesperrt werden. Es MUSS geprüft werden, welche Passwörter die ausscheidenden Mitarbeiter darüber hinaus noch kennen. Solche Passwörter MÜSSEN geändert werden.“

Durch die **rollenbasierte Zugriffskontrolle** können die Rechte bei Mitarbeiterwechseln umgehend entzogen werden. Es ist dokumentiert, auf welche Passwörter der Benutzer Zugriff hatte. Diese können auf einen neuen Wert zurückgesetzt werden. Zudem funktioniert Password Safe nach dem **Minimalprinzip**, der Benutzer kennt also nur so viele Passwörter wie nötig. Diese können zusätzlich durch den **Sichtschutz** gesichert werden.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.de
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE