PASSWORD SAFE

IT-Security im Gesundheitssektor

Die Bedeutsamkeit zuverlässiger wie hochverschlüsselter Zugangsverwaltung hat im **Gesundheitswesen** in den vergangenen Jahren so stark wie in kaum einer anderen Branche zugenommen. Ursache dafür sind unter anderem die Einführung der Datenschutz-Grundverordnung (DSGVO) sowie diverse Berichte über Cyberangriffe und Datendiebstähle. Dazu kommt: Datenzugänge im Gesundheitswesen werden oft mit besonders hohen Anforderungsprofilen und Verordnungen wie KRITIS konfrontiert. Um die Mitarbeiter in Krankenhäusern, Kliniken und Praxen nicht unnötig zu belasten, haben wir mit Password Safe eine zentrale Lösung zur einfachen wie sicheren Verwaltung und Nutzung von Zugangsdaten aller Art entwickelt.

Intelligente und sichere Lösungen für das Gesundheitswesen

Password Safe unterstützt dich mit einer individuell auf dein Unternehmen zugeschnittenen Passwortverwaltungslösung. Egal, ob es sich um verzweigte Berechtigungsstrukturen für Krankenhäuser oder um das zentrale Password Management in Arztpraxen handelt: Vertrauen Sie auf unsere umfangreiche Erfahrung und lange Expertise in der IT-Security-Branche!

Spare Zeit und Kosten und arbeite von Anfang an mit dem Marktführer im Bereich Password Management zusammen!

Passwort-Sicherheit ohne Grenzen

Ob Beside-Terminal, Patienten-Tablet oder Krankenhausinformationssystem (KIS): Der Zugriff auf alle Zugangsdaten erfolgt zentral und geräteübergreifend über die Web-Anwendung. Auch über Standorte, Stationen und Plattformen hinweg können Passwörter sicher – auch mit Externen – geteilt werden. Das sorgt für kürzere Bearbeitungswege und mehr Effizienz in den Arbeitsabläufen.

Einhaltung von Sicherheitsstandards

Um kritische Infrastrukturen (KRITIS) wie Krankenhäuser und Strukturen für stationäre Versorgung, Arzneimittel & Impfstoffe und Labore besonders zu schützen, sind klar definierte Zugriffsrechte essentiell. Durch das Zero-Knowledge-Prinzip in Password Safe können Passwörter sogar geteilt werden, ohne diese im Klartext zu kennen.

Zudem erhält jeder Mitarbeiter auf seine Rolle bezogen nur die Zugriffsberechtigungen, die für seine tägliche Arbeit notwendig sind – innerhalb des benötigten Zeitraumes. Unbefugte werden durch RBAC automatisch ausgesperrt.

Sicherheit an erster Stelle

Das Thema Datensicherheit hat gerade in der Gesundheitsbranche eine immense Bedeutung. Durch den täglichen Umgang mit sensiblen Patientendaten muss gewährleistet sein, dass diese geschützt werden und nur für autorisierte Personen zugänglich sind. Ein zentrales Berechtigungsmanagement auf Zugangsdaten inklusive Zwei-Faktor-Authentifizierung, PKI und Single-Sign-on hilft Ihnen dabei, diesem Anspruch gerecht zu werden.

Durch die Hinterlegung eines zweiten Faktors zum Login am Arbeitsplatz wird zum Beispiel das Passwort mit der Mitarbeiterkarte kombiniert. Via Single-Sign-on kann sich der Mitarbeiter nach einmaliger Authentifizierung automatisch an Websites anmelden lassen – die manuelle Anmeldung entfällt. Dem Patientenrechtegesetz entsprechend kann zudem durch die Dokumentation aller Zugriffe nachgewiesen werden, wann, wem und aus welchem Grund der Zugriff auf persönlich identifizierende Informationen (PII) erteilt wurde.

Krankenhauszukunftsgesetz zur Förderung Ihrer IT-Sicherheit

Mit dem Krankenhauszukunftsgesetz stellt das Bundesministerium für Gesundheit seit 01.01.2021 für Krankenhäuser Fördermittel zur Verfügung, um bei der Digitalisierung und bei Maßnahmen zur IT-Sicherheit zu unterstützen. Gemäß des KHZG sind mindestens **15 Prozent der gewährten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit** zu verwenden.

Förderfähige Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit **müssen** eine oder eine Kombination der folgenden funktionalen Anforderungen erfüllen:

- **Prävention vor Informationssicherheitsvorfällen:** Mit Password Safe verhindern Sie Angriffe und Vorfälle durch schlechte Passwörter und deren unsachgemäße Verwaltung.
- **Detektion von Informationssicherheitsvorfällen:** Alle Aktionen in Password Safe werden dokumentiert und können im Nachgang revisionssicher nachvollzogen werden.
- **Abschwächung von Informationssicherheitsvorfällen:** Durch zusätzliche Sicherheitsmechanismen wie 2FA, Sicherheitsstufen, Mehr-Augenprinzip, uvm. werden potentielle Vorfälle im voraus abgeschwächt.
- **Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheitsvorfällen bzw. der Bedeutung von IT-/Cybersicherheit:** Durch Funktionen wie die Einhaltung von Passwortrichtlinien, die Anzeige der Passwortqualität, uvm. werden Mitarbeiter zu einem bewussteren Umgang mit Passwörtern angewiesen.

Warum Password Safe?

Erfahrung

MATESO hat sich seit **2006** auf professionelles Enterprise Password Management fokussiert. **21 der Top 40 DAX-Unternehmen** sowie mehr als **10.000** Anwender vertrauen in puncto Passwort-Schutz bereits auf Password Safe.

Umfassender Schutz

Mit dem Einfluss von über **20 Jahren Markterfahrung** ist die Lösung ganzheitlich auf die individuellen Sicherheitsanforderungen und -bedürfnisse von Unternehmen zugeschnitten. Alle Passwörter werden ganzheitlich im **Password Life Cycle** geschützt – vom Erstellen bis hin zum Archivieren dieser.

Made in Germany

Als Mitglied der TeleTrust Initiative **»IT-Security Made in Germany«** steht MATESO für vertrauenswürde IT-Sicherheitslösungen, die den Anforderungen des deutschen Datenschutzrechts genügen, **DSGVO-konform** genutzt werden können und keine versteckten Zugänge enthalten.

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

MATESO
PASSWORD SAFE