Regelungen zum Passwortschutz

Firmenname/ Arztpraxis

Sicherheitsrichtlinie

Stand: Datum

Verantwortlich:	
Dokumentenebene:	Sicherheitsrichtlinie
Erstellt von:	
Version:	
Prüfungsintervall:	
Letzte Prüfung:	

Änderungsverzeichnis

Version	Datum	Autor	Änderung	Begründung	Seite

Inhaltsverzeichnis

1 Vorwort 4

2 Ziel 4

3 Grundsätzliche Passwort-Vorgaben 4

3.1 Passwortformat 4

3.2 Passwortänderung 5

3.3 Umgang mit Passwörtern 5

3.4 Systemtechnische Vorgaben für Passwörter 5

4 Spezielle Regelungen für Administratoren 6

4.1 Generell 6

4.2 Benutzer mit sonstigen Administratorrechten 6

5 Passwortaudit 6

Inkraftsetzung und Umsetzung 7

1 Vorwort

Die vorliegende Dienstanweisung enthält die Regelungen zum Passwortschutz. Um eine ordnungsgemäße Nutzung aller Anwendungen sicherzustellen, sind verbindliche Authentifizierungsverfahren durch Eingabe von Benutzername und Passwort unerlässlich. Dies gilt insbesondere für zu schützende Informationen gemäß dem Bundesdatenschutzgesetz (BDSG) (personenbezogene Daten) und dem Sozialgesetzbuch X (SGB X) (Sozialdaten).

2 Ziel

Der Passwortschutz eines IT-Systems oder einer IT-Anwendung dient dazu, sicherzustellen, dass ausschließlich berechtigte Benutzer Zugriff auf Systeme, Daten und Anwendungen erhalten. Er gewährleistet, dass nur Personen Zugang erhalten, die ihre Identität durch ein gültiges Passwort nachweisen. Diese Maßnahme ist von zentraler Bedeutung, um Missbrauch durch unbefugte Dritte zu verhindern und die Sicherheit der IT-Infrastruktur zu gewährleisten

3 Grundsätzliche Passwort-Vorgaben

3.1 Passwortformat

(1) Passwörter müssen mindestens 12 Zeichen lang sein.

(2) Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdaten und ähnliche leicht zugängliche Informationen dürfen daher nicht als Passwort verwendet werden.

(3) Der Anmeldename oder mehr als zwei Zeichen, die nacheinander im vollständigen Namen des Benutzers enthalten sind, dürfen nicht als Passwort verwendet werden.

(4) Passwörter zur Anmeldung an Systemen bei PCs oder Notebooks müssen Zeichen aus mindestens 3 dieser 4 Gruppen enthalten:
- Kleinbuchstaben (a - z)
- Großbuchstaben (A - Z)
- Zahlen (0 - 9)
- Sonderzeichen (z. B. %, €, !, $, ')

(5) Jedes Passwort sollte einzigartig sein und nicht für mehrere Konten verwendet werden.

3.2 Passwortänderung

(1) Das Passwort darf grundsätzlich nur von der Person geändert werden, dessen Benutzerkennung mit diesem Passwort verbunden ist.

(2) Bevor ein Passwort durch den IT Helpdesk oder andere Personen zurückgesetzt/geändert wird, ist die Identität des betroffenen Benutzers zu prüfen.

(3) Startpasswörter, die durch den IT Helpdesk oder andere Personen vergeben wurden, müssen bei der erstmaligen Verwendung sofort durch den Anwender geändert werden.

(4) Das Passwort muss alle 90 Tage gewechselt werden.

(5) Neue Passwörter dürfen nicht mit den zehn vorhergehenden übereinstimmen.

(6) Das minimale Passwortalter zur Anmeldung an PCs oder Notebooks beträgt 3 Tage. Sollte ein Passwort in diesem Zeitraum kompromittiert werden, so ist die Änderung des Passworts über den IT Helpdesk zu veranlassen.

(7) Die Eingabe des Passwortes muss unbeobachtet und durch den Inhaber des Benutzerkontos selbst stattfinden.

(8) Bei Eingabe eines Passwortes darf dieses nicht lesbar am Bildschirm angezeigt werden.

(9) Nach 5 ungültigen Anmeldeversuchen an Betriebssystemen wird das entsprechende Berechtigungskonto des Anwenders maschinell gesperrt! Diese Sperre wird nach Zeitablauf von 30 Minuten automatisch wieder aufgehoben. Sollte ein Berechtigungskonto vor diesem Zeitablauf entsperrt werden, so ist der Helpdesk zu verständigen.

(10) Ein außerordentlicher Passwortwechsel ist durchzuführen, wenn das Passwort anderen Personen bekannt geworden ist oder ein entsprechender Verdacht besteht.

3.3 Umgang mit Passwörtern

(1) Den Mitarbeitern ist es ausdrücklich untersagt, ihre Passwörter gegenüber Dritten, gleichgültig ob Kollegen oder Externe, bekannt zu machen.

(2) Weiterhin dürfen Passwörter weder aufgeschrieben und am Arbeitsplatz verwahrt noch unverschlüsselt auf IT-Systemen oder anderen Speichermedien gespeichert werden.

(3) Passwörter dürfen nicht auf programmierbaren Funktionstasten usw. gespeichert werden.

(4) Jedes Passwort sollte einzigartig sein und nicht für mehrere Konten verwendet werden.

3.4 Systemtechnische Vorgaben für Passwörter

(1) Passwörter sind im Computersystem nur verschlüsselt zu speichern.

(2) Eine eventuell vorhandene Passwortdatei ist gegen unberechtigtes Kopieren zu schützen.

(3) Anmeldefehlversuche an einem System sind, sofern es das System zulässt, zu protokollieren.

4 Spezielle Regelungen für Administratoren

4.1 Generell

(1) Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.

(2) Benötigen Dienste auf Servern zusätzliche Accounts mit Administratorrechten, müssen auch diese Accounts mit einem 15-stelligen Passwort gesichert und zentral hinterlegt werden. Dies gilt ebenso für betriebsrelevante Passwörter, wie etwa für Systemkomponenten, Netzwerkgeräte, Lizenzdaten und den Login bei Softwareanbietern wie VMware, Microsoft und anderen

(3) Mit Ausnahme der Regelungen unter 4.1 und 4.2 gelten allen anderen Regelungen (3.1 bis 3.4) entsprechend.

4.2 Benutzer mit sonstigen Administratorrechten

(1) Passwörter müssen mindestens 15 Stellen lang sein.

(2) Das Passwort muss alle 90 Tage gewechselt werden.

5 Passwortaudit

Alle vier Wochen sollen regelmäßige Passwort-Audits* durchgeführt werden, um kompromittierte Passwörter zu identifizieren. Betroffene Benutzer sind per E-Mail oder telefonisch zu benachrichtigen und aufzufordern, ihr Passwort innerhalb von zwei Tagen zu ändern. Erfolgt die Änderung nicht innerhalb der Frist, ist der IT ServiceDesk berechtigt, das Passwort ohne weitere Rücksprache zu ändern. In diesem Fall wird der Benutzer beim nächsten Anmeldevorgang dazu aufgefordert, ein neues Passwort festzulegen.

* Tools wie Specops Password Auditor sind kostenlos und unterstützen dabei, kompromittierte Passwörter zu identifizieren

Inkraftsetzung und Umsetzung

Die Richtlinie „Regelungen zum Passwortschutz nach IT-Grundschutz (BSI)" ist für alle Beschäftigten verbindlich.

Sollten die Regelungen aufgrund technischer oder organisatorischer Besonderheiten nicht vollständig umgesetzt werden können, sind sie sinngemäß anzuwenden.

Verstöße gegen diese Richtlinien werden besonders ernst genommen und können arbeitsrechtliche oder dienstrechtliche Konsequenzen nach sich ziehen.

Diese Richtlinie tritt mit sofortiger Wirkung in Kraft

_____

Geschäftsleitung