



Dienstanweisung Nr. 51/2016 zur Regelung des Passwortgebrauches

Inhalt

§ 1 Zielsetzung	3
§ 2 Geltungsbereich	3
§ 3 Grundsätze für die Administration.....	3
§ 4 Regelungen für die Benutzer	4
§ 5 Outlook Web Aaccess sowie externer Intranet-Zugang	5
§ 6 Passworte von Fachanwendungen	5
§ 7 Inaktive Benutzerkonten	5
§ 8 Inkrafttreten	5

§ 1 Zielsetzung

Passwörter dienen der Authentifizierung (Nachweis der Identität). Die Verwendung von sicheren Passwörtern und deren korrekte Nutzung vermindern in der Informationssicherheit die Risiken in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität.

§ 2 Geltungsbereich

(1) Die Dienstanweisung gilt für tariflich Beschäftigte, Beamte, Auszubildende und Praktikanten des Landkreises Teltow-Fläming, nachfolgend Beschäftigte genannt, sowie für alle weiteren Personen denen ein Nutzungsrecht der Informationstechnik eingeräumt wird.

2) Der/die Sachgebietsleiter/-in nimmt als unmittelbare/-r Vorgesetzte/-r die sich aus dieser Dienstvereinbarung ergebenden Führungsaufgaben wahr. Soweit der/die unmittelbare Vorgesetzte nicht Sachgebietsleiter/-in ist, gelten die Zuständigkeiten für den/die Amtsleiter/-in, den/die Dezernent/-in, den/die Landrat/Landrätin entsprechend.

§ 3 Grundsätze für die Administration

(1) Der unmittelbare Zugang zum Netz der Kreisverwaltung Teltow-Fläming und zu den Fachanwendungen erfolgt über persönliche Passwörter der Beschäftigten.

(2) Jedes System oder Programm, welches sensible Daten verarbeitet, muss durch eine Benutzerkennung und einem dazugehörigen Passwort gesichert werden.

(3) Benutzerkennung und Startpasswort werden telefonisch, persönlich oder verschlossen in einem Umschlag übergeben.

(4) Der Passwortwechsel wird vom Betriebssystem und den Fachanwendungen regelmäßig initiiert. Dies hat mindestens alle 90 Tage zu geschehen.

(5) Die Wahl von Trivialpasswörtern (z. B. "BBBBBBBB", "123456") wird verhindert.

(6) Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass ein Passwort nicht in kurzer Zeit durch einfaches ausprobieren ermittelt werden kann.

(7) Die Passwörter werden im System zugriffssicher gespeichert, z. B. mittels Einweg-Verschlüsselung (Hashfunktionen).

(8) Der Zugang zum IT-Hausnetz der Kreisverwaltung wird nach dreifacher fehlerhafter Passwordeingabe gesperrt. Die erneute Freigabe der Kennung erfolgt durch autorisierte Beschäftigte des IT-Service (Service-Hotline).

(9) Bei einer Inaktivität von 20 Minuten wird die Bildschirmsperre automatisch aktiviert, sodass eine erneute Anmeldung nur mit Passwort möglich ist.

(10) Für die Erstanmeldung neuer Benutzer werden Einmalpasswörter vergeben, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.

(11) Alte Passwörter dürfen frühestens nach dem fünften Passwortwechsel wieder gebraucht werden. Die Wiederholung alter Passwörter soll verhindert werden.

(12) Bei der Eingabe darf das Passwort nicht auf dem Bildschirm angezeigt werden.

(13) Die Beschäftigten können ihre individuellen Passwörter jederzeit ändern.

(14) Passwörter für Programme, welche personenbezogene und sensible Daten verarbeiten, dürfen über ein ungesichertes Netz hinweg nicht unverschlüsselt übertragen werden.

§ 4 **Regelungen für die Benutzer**

(1) Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist. Folgende Eigenschaften müssen vermieden werden:

- Zeichenwiederholungen,
- Zahlen und Daten aus dem persönlichen Lebensbereich,
- einfache Ziffern- und Buchstabenkombinationen,
- Zeichenketten wie „qwertzu!“, die durch nebeneinander liegende Tasten eingegeben werden,
- Zeichenkombinationen, die Suchbegriffen in Wörterbüchern oder Lexika entsprechen.

Innerhalb des Passwortes (mindestens 8 Zeichen lang) sind Groß- und Kleinbuchstaben sowie mindestens ein Zeichen, das kein Buchstabe ist (Sonderzeichen oder Zahl) zu verwenden.

(2) Bei Verlassen des Arbeitsplatzes ist Computersperre/Bildschirmsperre zu aktivieren (Windows-Taste + L).

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

(4) Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.

(5) Das Passwort darf nur dem Benutzer persönlich bekannt sein. Es darf nicht an andere weitergegeben werden. Die Aufforderung zur Weitergabe des Passwortes ist untersagt. Wird das Passwort vergessen, kann eine Zurücksetzung erfolgen.

(6) Es ist sicherzustellen, dass die Eingabe des Passwortes unbeobachtet stattfindet.

(7) Besteht der Verdacht, dass Passwörter nichtautorisierten Personen bekannt geworden sind, sind diese unverzüglich zu ändern.

(8) Passwörter von Webseiten im Webbrowser sind auf den lokalen Rechnern nicht zu speichern, das dauerhafte Aktivieren einer Anmeldung ist nicht zulässig.

§ 5

Outlook Web Access sowie externer Intranet-Zugang

Das Passwort für Zugriff auf den verschlüsselten Outlook Web Access sowie den Intranet-Zugang aus ungesicherten Netzen wird alle 6 Monate (zum 01.05. sowie 01.11. des Jahres) zentral geändert. Beschäftigte erhalten das neue Kennwort auf Nachfrage vom IT-Service über die Service-Hotline.

§ 6

Passworte von Fachanwendungen

Sind die Regelungen aus Paragraf 3 in Fachanwendungen und Hilfsprogrammen technisch nicht umsetzbar, ist durch organisatorische Regelungen (Arbeitsanweisungen) das Sicherheitsrisiko zu minimieren. Die organisatorischen Maßnahmen sind durch die Sachgebietsleiter/-innen festzulegen, zu dokumentieren und dem IT-Sicherheitsbeauftragten vorzulegen.

§ 7

Inaktive Benutzerkonten

Bei Bekanntwerden der Beendigung des Beschäftigungsverhältnis bzw. einer Umsetzung wird der IT-Service unverzüglich durch das Sachgebiet Personal und Organisation durch ein Ticket über den Termin informiert, so dass eine Deaktivierung und Abwicklung / Anpassung des Benutzerkontos termingerecht realisiert werden kann.

Der/die Sachgebietsleiter/-in sorgt dafür, dass Fachverfahren-Benutzerkonten regelmäßig auf inaktive Nutzung überprüft werden und eine regelmäßige Aktualisierung initiiert wird. Inaktiv bedeutet in diesem Fall auch, wenn sich die Arbeitsaufgaben oder die fachliche Zuständigkeit ändert und somit ein Zugriff auf das System nicht mehr benötigt wird.

§ 8

Inkrafttreten

Diese Dienstanweisung tritt am 1. Mai 2016 in Kraft.

Luckenwalde, den 19.04.2016

Wehlan
Landrätin