Passwortrichtlinie

Inhaltsverzeichnis

§ 1 Geltungsbereich

§ 2 Pflichten des Systemmanagements und der Programmentwicklung

§ 3 Pflichten der Passwortverwaltung

§ 4 Pflichten der Benutzer

§ 5 Verfahren der automatisierten Passwortrücksetzung

§ 6 Weitere Maßnahmen

§ 7 Ausnahmeregelungen

§ 8 Inkrafttreten

Verantwortliche Stelle: Name

Strasse / Hausnummer

PLZ / Stadt

§ 1 Geltungsbereich

(1) Die Richtlinie regelt die Vergabe und die Handhabung von Passwörtern, die zur Identitätsüberprüfung der Benutzer eingesetzt werden.
(2) Die Richtlinie gilt für alle IT-Systeme und Kommunikationssysteme, deren Daten durch Passwörter vor unbefugtem Zugriff Dritter geschützt werden sollen.

§ 2 Pflichten des Systemmanagements und der Programmentwicklung

(1) Die Passwortdateien sind vor unbefugten Zugriffen zu schützen.
(2) Die Software ist im Rahmen des technischen Standes so zu gestalten, dass folgendes überprüft und sichergestellt ist: Die Passwörter sind aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammengesetzt. Die Passwörter sind aus einer Mindestlänge von 8 Stellen zusammengesetzt. Passwörter, die leicht zu erraten sind oder in einem Sinnzusammenhang stehen, sind nicht vergeben. Die Passwörter sind während der Eingabe nicht lesbar am Bildschirm zu erkennen. Das Benutzerkonto ist nach 5-maliger fehlerhafter Passworteingabe zu sperren. Benutzerkonten, die länger als 90 Tage nicht aktiviert wurden, sind zu sperren. spätestens nach 180 Tagen ist ein Wechsel der Passwörter zu betreiben. Die Passwörter sind dem Stand der Technik entsprechend nur einwegverschlüsselt zu speichern. Die Passwörter sind nur verschlüsselt im Netzwerk zu übertragen.
(3) Handelt es sich um nicht schutzbedürftige Daten oder Passwörter, die nicht zum Authentifizieren dienen, kann von den eben genannten Punkten 1. bis 9. abgewichen werden.
(4) Soweit es sich um besonders schutzbedürftige Daten handelt, ist eine Mindestlänge von 12 Stellen und eine kürzere Geltungsdauer als 180 Tage festzusetzen. Bei dieser Bestimmung ist sowohl der potentielle Schaden im Falle unbefugter Nutzung, als auch dessen Risiko zu beachten.

(5) Bei Softwareinstallation erstellte oder anderweitig automatisch vergebene Passwörter sind
unverzüglich durch neue zu ersetzen.
(6) Alle Falscheingaben der Passwörter sind zu dokumentieren. Die Protokolle sind stets auszuwerten. Sollte ein Benutzer nach 5-maliger Eingabe gesperrt werden, so ist die Sperre erst nach erfolgreicher Identitätsprüfung aufzuheben.

§ 3 Pflichten der Passwortverwaltung
(1) Das von der Verwaltung vergebene Übergangspasswort ist so weiterzugeben, dass eine Kenntnisnahme durch unbefugte Dritte vermieden wird. Der empfangende Benutzer ist aufzufordern, das Übergangspasswort unverzüglich in ein eigenes, den Vorgaben dieser Richtlinie entsprechendes Passwort zu ändern.
(2) Wurde der Zugang des Benutzers nach mehrmaliger Falscheingabe des Passwortes gesperrt, so ist vor der Freischaltung dessen Identität zu überprüfen und zu dokumentieren.
(3) Blieb die automatisierte Passwortrücksetzung erfolglos, so ist die Rücksetzung auf Antrag des Berechtigten durch die für die Passwortverwaltung zuständige Stelle zu veranlassen. Dabei ist die Identität des Berechtigten zu überprüfen und zu dokumentieren.
(4) Sollte eine angeforderte Passwortneutralisierung nicht von dem Inhaber des Benutzerkontos selbst veranlasst worden sein, ist dieser davon in Kenntnis zu setzen und zur unverzüglichen Änderung des Passwortes aufzufordern.
(5) Benutzerkennungen, die veraltet sind oder länger nicht genutzt wurden, sind zu sperren.

§ 4 Pflichten der Benutzer
(1) Die Passwörter sind geheim zu halten. Sie dürfen vor allem nicht unverschlüsselt auf dem Rechner oder offen auf dem Arbeitsplatz hinterlegt werden. Bei der Eingabe des Passwortes ist ebenfalls darauf zu achten, dass sie geheim erfolgt.
(2) Alle in Nutzung stehenden Geräte sind mit automatischen Bildschirmabschaltungen auszustatten, die nach einer an der Schutzwürdigkeit der Daten orientierten Zeit das Passwort abfragen und einen unbefugten Zugriff verhindern.
(3) Bei der Passwortvergabe sind mindestens 8, besser jedoch 12 Stellen zu belegen.
(4) Passwörter sind technisch so komplex wie möglich aus Groß- und Kleinbuchstaben, Zahlen und Zeichen zusammenzusetzen.
(5) Folgendes darf nicht verwendet werden: sinnbringende Wörter, die bspw. auch in einem Wörterbuch zu finden sind in Zusammenhang stehende einfache Zahlen- und Buchstabenkombinationen Zahlen und Buchstaben, die auf der Tastatur nebeneinander liegen, Wiederholungen, Angaben und Daten aus dem persönlichen Umfeld ein Passwort, das nur unwesentlich von einem vorherigen abweicht
(6) Die Passwörter sind spätestens nach 180 Tagen zu wechseln. Erlangt ein Dritter Kenntnis von einem Passwort, so ist es jedoch unverzüglich zu ändern. Auch ein bloßes Verdachtsmoment genügt hierfür.
(7) Von der Systemverwaltung zu Beginn vergebene Passwörter oder Übergangspasswörter sind unverzüglich durch ein eigenes, dieser Richtlinie entsprechendes Passwort zu ersetzen.

§ 5 Verfahren der automatisierten Passwortrücksetzung
(1) Für die Passwortrücksetzung ist ein automatisiertes Verfahren anzuwenden, wenn technische und organisatorische Möglichkeiten dies erlauben. Dazu ist im Vorfeld jeweils ein Masterpasswort nach den Vorgaben dieser Richtlinie zu erstellen, was bei einer Passwortrücksetzung den Benutzer authentifiziert.
(2) Der Datenschutzbeauftragte ist bei Einführung eines automatisierten Verfahrens zu kontaktieren.

§ 6 Weitere Maßnahmen
(1) Die Einhaltung der Richtlinie ist durch geeignete organisatorische und technische Maßnahmen sicherzustellen.
(2) Alle Beschäftigten sind über den Inhalt dieser Richtlinie zu informieren und zu schulen. Die tatsächliche Kenntnisnahme ist prüfen.
(3) Benutzerkennungen sind personenbezogen zu vergeben.
(4) Auch anderweitige Authentifizierungsmittel (wie bspw. Chipkarten oder Token) sind ebenfalls so zu verwalten, dass auf sie keine unbefugten Dritten zugreifen können.

§ 7 Ausnahmeregelungen
Es sind Ausnahmegenehmigungen von dieser Richtlinie zu erteilen, wenn die Grundsätze des Datenschutzes und der Datensicherheit nicht beeinträchtigt werden, der IT- Infrastruktur keine Gefahr droht und ein Datenschutzbeauftragter einbezogen wird.

§ 8 Inkrafttreten
Diese Passwortrichtlinie tritt unmittelbar an folgendem Datum in Kraft: XX.XX.XXXX