IT-Handbuch

für die Verwaltung der
Freien und Hansestadt Hamburg

Richtlinie zur Verwaltung von Passwörtern

(Passwortrichtlinie - Passwort-RL)

vom 10.10.2007 (MittVw Seite 96)

1. Geltungsbereich

(1) Diese Richtlinie regelt die Gestaltung und Handhabung von Passwörtern, die zur Authentisierung berechtigter Benutzer eingesetzt werden.

(2) Sie ist im Rahmen der technischen Möglichkeiten auf alle IuK-Systeme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen. Auf Telekommunikationseinrichtungen ist sie anzuwenden, soweit dem nicht technische Einschränkungen entgegenstehen.

2. Pflichten der Benutzer

(1) Passwörter sind geheim zu halten. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden.

(2) Die Länge der Passwörter richtet sich nach dem Schutzbedarf der Daten und Ressourcen. Sie beträgt mindestens 8 Stellen. Benutzerkennungen mit besonderen Rechten und Aufgaben (z.B. Systemverwaltung, Sicherheitsfunktionen oder Anwendungen mit sensiblen Daten) sind mit Passwörtern zu schützen, die mehr als 8 Zeichen umfassen (s. Abschnitt 6 Abs. 1)

(3) Passwörter sollen technisch so komplex wie möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). Dies ist der wesentlichste Schutz vor systematischem Ausspähen.

(4) Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere:

1. Zeichenwiederholungen,
2. Zahlen und Daten aus dem Lebensbereich des Benutzers,

3. Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen,

4. einfache Ziffern- und Buchstabenkombinationen,

5. Zeichen, die durch nebeneinander liegende Tasten eingegeben werden.

6. Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter).

(5) Passwörter sind nach einer dem Schutzbedarf der Daten und Ressourcen angemessenen Frist, mangels weitergehender Bestimmungen (Abschnitt 5 Absatz 1) spätestens nach 90 Tagen zu wechseln.

(6) Passwörter dürfen in der Regel höchstens einmal am Tag gewechselt werden. Sie sind jedoch unverzüglich zu wechseln, wenn der Verdacht besteht, dass sie Dritten bekannt geworden sein könnten.

(7) Einstiegs- und Übergangspasswörter sind unverzüglich durch eigene Passwörter zu ersetzen.

(8) Endgeräte sind mit passwortgeschützten Bildschirmschonern bzw. Bildschirmabschaltungen zu versehen, die je nach Schutzwürdigkeit der Daten und Ressourcen nach einer bestimmten Zeit den Zugriff auf das angemeldete Endgerät verhindern. Für die Entsperrung mittels Passwort gelten die Regeln dieser Richtlinie entsprechend.

3. Pflichten der Systemverwaltung und Programmentwicklung

(1) Passwortdateien sind vor unbefugtem Zugriff zu schützen.

(2) Bei der Softwareinstallation automatisch vergebene Passwörter sind unverzüglich durch neue zu ersetzen.

(3) Passwörter, die nicht im Zusammenhang mit dem Anmelden (Login) einzugeben sind (anwendungsbezogene Passwörter), orientieren sich hinsichtlich der Länge der verwendeten Zeichen und der Frist für einen Passwortwechsel am Schutzbedarf der Anwendung und der zu verarbeitenden Daten. Besteht kein zusätzlicher Schutzbedarf, kann von den Vorgaben nach Nummer 2 Absätze 3 bis 5 abgewichen werden.

(4) Software ist so zu gestalten bzw. grundsätzlich so zu konfigurieren, dass Benutzer nur Passwörter mit einer Mindestlänge von 8 Zeichen vergeben können. Vorgaben für anwendungsbezogene Passwörter haben den jeweiligen Schutzbedarf der Anwendung zu beachten.

(5) Fehlversuche bei der Passworteingabe sind zu protokollieren. Die Protokolle sollen regelmäßig ausgewertet werden.

(6) Soweit möglich, ist durch softwaretechnische Maßnahmen vorzugeben, dass

1. nur Passwörter vergeben werden können, die aus der größtmöglichen Zeichenmischung von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen zusammengesetzt sind,

2. nach der vorgegebenen Frist, spätestens nach 90 Tagen, ein Passwortwechsel erzwungen wird,

3. Benutzerkennungen, die länger als 45 Tage nicht aktiviert wurden, gesperrt werden,

4. Passwörter nicht am Bildschirm angezeigt werden,

5. Passwörter einwegverschlüsselt gespeichert werden,

6. nach 5maliger fehlerhafter Passworteingabe die Benutzerkennung gesperrt und die Systemadministration informiert wird,

7. Passwörter in Netzwerken verschlüsselt übertragen werden und

8. leicht zu erratende Passwörter nicht vergeben werden können.

(7) Ist die Sperrung der betroffenen Benutzerkennungen nach 5maliger fehlerhafter Passworteingabe nicht möglich oder sinnvoll, sind andere gleichwertige Maßnahmen zu treffen (z.B. Zeitverzögerungen zwischen den möglichen Eingabeversuchen).

(8) Bei der Auswahl von IuK-Systemen ist auf die Verfügbarkeit entsprechender Mechanismen zu achten. Sofern diese auf Ebene der Betriebssysteme oder der Anwendung nicht verfügbar sind, ist der Einsatz geeigneter Zusatz-Software erforderlich.

4. Verfahren für die automatisierte Passwortrücksetzung

(1) Soweit technisch und organisatorisch möglich wird für die Passwortrücksetzung ein automatisiertes Verfahren eingesetzt. Dabei haben die Nutzer des automatisierten Verfahrens im Vorwege mehrere selbst ausgewählte Fragen aus einem Fragenkatalog zu beantworten. Die angegebenen Antworten bzw. Zeichenkombinationen dienen zur späteren Authentisierung des Nutzers und sind deshalb geheim zu halten. Folgende Kriterien sind bei der Einrichtung eines automatisierten Verfahrens zu beachten:

1. Der Nutzer muss mindestens 3 Fragen aus einem Fragenkatalog beantworten,

2. die Fragen und Antworten sind einwegverschlüsselt zu speichern,

3. bei der Eingabe möglicher Antworten steht der gesamte Zeichenvorrat zur Verfügung (Sonderzeichen, Groß- und Kleinschreibung).

(2) Möchte der Nutzer über ein automatisiertes Verfahren Zugriff zu Verfahren im FHHNET bzw. zur Windows-Benutzeroberfläche erlangen, kann er sein Passwort unter Beachtung der nachfolgenden Verfahrensschritte selbständig zurücksetzen:

1. Beantwortung der Fragen mit den Antworten bzw. Zeichenkombinationen, die der Nutzer für das automatisierte Verfahren hinterlegt hat. Über die erforderlichen Verfahrensschritte wird der Nutzer im Vorwege informiert.

2. Nach korrekter Beantwortung der ausgewählten Fragen wird der Nutzer im Rahmen einer technischen Vorgabe (siehe auch Nr. 2 (7)) aufgefordert, für seinen Account ein neues Passwort einzugeben.

(3) Vor Einführung eines automatisierten Verfahrens ist der behördliche Datenschutzbeauftragte zu informieren. Ist ein solcher nicht bestellt oder handelt es sich um ein behördenübergreifendes Verfahren, ist der Hamburgische Datenschutzbeauftragte zu informieren.

5. Pflichten der für die Passwortverwaltung Zuständigen

(1) Sollte eine automatisierte Passwortrücksetzung erfolglos bleiben oder nicht zur Verfügung stehen, muss die Passwortrücksetzung über einen Auftragsberechtigten erfolgen. Dabei hebt auf Antrag eines Berechtigten die für die Passwortverwaltung zuständige Stelle die Sperre einer Benutzerkennung auf oder neutralisiert ein Benutzerpasswort, wenn sie sich von der Identität des Berechtigten überzeugt hat. Berechtigt sind der Inhaber der betroffenen Benutzerkennung, der zur Autorisierung von Benutzern Berechtigte oder, wenn dieser nicht bestimmt wurde, der jeweilige Amtsleiter. Wurde die Sperre einer Benutzerkennung von einem zur Autorisierung von Benutzern Berechtigten bzw. dem Amtsleiter verfügt, darf die Passwortverwaltung sie nur auf dessen Auftrag hin zurücknehmen.

(2) Das Aufheben der Sperre und die Passwortneutralisierung sind revisionssicher zu dokumentieren, so dass nachvollziehbar ist, wer der Auftraggeber war und wie seine Berechtigung und Identität geprüft wurde.

(3) Ein von der Passwortverwaltung vergebenes Übergangspasswort (z.B. bei der Entsperrung oder der Passwortneutralisierung) ist so mitzuteilen, dass eine Kenntnisnahme durch Unbefugte vermieden wird. Zugleich ist der Empfänger des Übergangspasswortes aufzufordern, das Übergangspasswort unverzüglich zu ändern.

(4) Der Inhaber der Benutzerkennung ist von einer Passwortneutralisierung zu informieren, wenn sie nicht von ihm veranlasst wurde. Zugleich ist der Inhaber aufzufordern, das neutralisierte Passwort unverzüglich zu ändern.

(5) Nicht mehr benötigte oder für einen längeren Zeitraum nicht genutzte Kennungen sind zu sperren, außer es ist für die Funktionsfähigkeit des Betriebes als solchen notwendig, dass die Kennung nicht gesperrt werden kann. Dies gilt auch für entsprechende Wartungs- und Fernwartungskennungen.

6. Organisatorische Maßnahmen

(1) Soweit der Schutzbedarf der Daten und Ressourcen es erfordert, ist für die Passwörter eine angemessene Länge von mehr als 8 Stellen und eine kürzere Gültigkeitsdauer als 90 Tage festzulegen. Bei der Festlegung der angemessenen Gültigkeitsdauer sind insbesondere der potentielle Schaden zu berücksichtigen, der entstünde, wenn ein

Unbefugter das Passwort über einen längeren Zeitraum nutzen würde, sowie das Risiko, das ein Unbefugter das Passwort noch längere Zeit nach Kenntnisnahme nutzen könnte.

(2) Die Einhaltung dieser Richtlinie ist durch geeignete Maßnahmen im Rahmen der Dienstaufsicht sicherzustellen.

(3) Die Beschäftigten sind entsprechend den Erfordernissen - mindestens aber einmal jährlich - über den Inhalt dieser Richtlinie zu informieren.

7. Sonstige Maßnahmen

(1) Benutzerkennungen sollen personenbezogen vergeben werden.

(2) Werden andere Authentisierungsmittel als Passwörter eingesetzt (z.B. Magnet-, Chipkarte), müssen sie so gehandhabt werden, dass die Benutzung durch Unbefugte ausgeschlossen ist. Soweit erforderlich, treffen die zuständigen Stellen hierzu besondere Regelungen.

8. Ausnahmeregelungen

Die für Grundsatzangelegenheiten der IuK-Technik zuständige Behörde kann Ausnahmegenehmigungen von dieser Richtlinie erteilen, wenn die Grundsätze des Datenschutzes und der Datensicherheit eingehalten werden und keine Gefahr für die IuK-Infrastruktur besteht. Dabei sind die §§ 8 und 9 des Hamburgischen Datenschutzgesetzes zu beachten, insbesondere die Verfahrensbeschreibung und die Risikoanalyse anzupassen, sowie der Hamburgische Datenschutzbeauftragte zu beteiligen.

9. Inkrafttreten

Diese Richtlinie tritt am 10.10.2007 in Kraft. Zum gleichen Zeitpunkt tritt die Richtlinie zur Verwaltung von Passwörtern vom 01.03.2007 (MittVw 2007 Seite 22) außer Kraft.