B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

Passwortrichtlinie Vorlage

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Passwortrichtlinie

der Muster GmbH, Musterstr. 123, 12345 Musterhausen

Anwendungsbereich der Passwortrichtlinie

1. Diese Passwortrichtlinie regelt die Gestaltung und die Handhabung der Passwörter, die zur Authentisierung von berechtigten Benutzer verwendet werden.
2. Sie ist im Rahmen der technischen Möglichkeiten auf alle EDV-Systeme anzuwenden, deren Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und damit verbundener missbräuchlicher Verwendung oder Veränderung geschützt werden müssen.
3. 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.

Regeln für die Benutzer zum Umgang mit Passwörtern

1. Benutzer müssen die Geheimhaltung ihrer Passwörter sicherstellen. Die Eingabe von Passwörtern muss verdeckt erfolgen. Untersagt ist insbesondere folgender Umgang mit Passwörtern:
   - Unverschlüsselt auf Rechnern speichern.
   - Auf Funktionstasten hinterlegen.
   - Auf einem Notizzettel aufschreiben.
   - An Kollegen weitergeben, zum Beispiel bei Urlaubsvertretung.
   - Immer das gleiche Passwort für alle internen und externen Anwendungen verwenden.
   - Notfallpasswörter ungeschützt hinterlegen.
2. Die Stärke des Passworts sollte nach dem Schutzbedarf der Daten und Ressourcen gewählt werden. Folgende Regeln sollten bei der Festlegung von Passwörtern berücksichtigt werden:
   - Es sind keine Passwörter mit weniger als 8 Zeichen zulässig.
   - Passwörter, die für Sicherheitsfunktionen oder dem Schutz von Anwendungen mit sensiblen Daten verwendet werden, müssen mindestens 12 Zeichen umfassen.
   - In den Passwörtern sollte mindestens benutzt werden: Ein Kleinbuchstabe (z.B. „a“), ein Großbuchstabe (z.B. „C“), eine Ziffer (z.B. „5“) und ein Sonderzeichen (z.B. „%“).
   - Je länger ein Passwort, desto sicherer ist dies. Die Ableitung von einem Anagramm hilft bei der Passwortbildung (z.B. der Satz „Mein erster größter Wunsch im Leben ist eine sichere Zukunft ohne Krieg und Zerstörung!“ ergibt folgendes Passwort: M1.gWiLiesZoKuZ!)

3. Um zu verhindern, dass Passwörter zu leicht erraten werden können, ist folgendes nicht zulässig:
   - Einfache Ziffern- und Buchstabenkombinationen oder mehrfache Wiederholung der selben Zeichen.
   - Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden (z.B. „QWERTZUI“ oder „12345678“).
   - Zahlen und Begriffe, die aus den bekannten Lebensumständen des Benutzers abgeleitet werden können (z.B. Namen von Haustieren, Wohnort, Kfz-Kennzeichen, Geburtsdaten, …).
   - Trivialpasswörter aus Zeichenkombinationen, die typischen Suchbegriffen in Wörterbüchern und Lexika entsprechen.
   - Kombinationen aus Zeichen, die im vorher benutzen Passwort verwendet wurden oder nur unwesentlich abweichen.
4. Der Wechsel von Passwörtern hat nach einer dem Schutzbedarf der Daten und Ressourcen angemessenen Frist zu erfolgen (als Richtwert sollten 180 Tage nicht überschritten werden). Besteht der Verdacht, dass ein Passwort einem Dritten bekannt wurde, ist es unverzüglich zu wechseln und der zuständige Administrator ist zu informieren.

5. Ein Einstiegs- oder Übergangspasswort ist sofort durch ein eigenes Passwort zu ersetzen.
6. Zum Erzeugen von Passwörtern darf ein von der EDV-Administration zugelassener Passwortgenerator (z.B. KeePass) eingesetzt werden.

Pflichten von Administratoren bzw. der für die Passwortverwaltung zuständigen Mitarbeiter

1. Die Passwortdateien der Benutzer sind vor unbefugtem Zugriff zu schützen (siehe technisch-organisatorische Maßnahmen).
2. Benutzerkennungen sollen personenbezogen vergeben werden (nicht „rollenbezogen“ für mehrere Personen).
3. Werden Passwörter bei der Installation von Software automatisch vergeben, sind diese sofort zu ersetzen.
4. Für die Sicherheit sonstiger anwendungsbezogener Passwörter, die nicht im Zusammenhang mit dem Anmelden (Login) einzugeben sind, gelten die gleichen Vorgaben hinsichtlich der Festlegung: Die Anzahl der Zeichen sowie die Frist für einen Passwortwechsel muss sich am Schutzbedarf der Anwendung und der damit verarbeiteten Daten orientieren. Für Anwendungen ohne Schutzbedarf kann von den Vorgaben abgewichen werden.

5. Die Aufhebung einer Passwortsperre ist nur dann möglich, wenn die Identität des Berechtigten eindeutig nachgewiesen wurde. Das Aufheben einer Sperrung und die Passwortneutralisierung sind veränderungssicher zu dokumentieren.

Technisch organisatorische Maßnahmen

1. Passwortdateien dürfen nur mittels geeigneter Software bzw. praktikablen Verfahren gespeichert werden. Dies können Password Manager (z.B. KeePass) oder passwortgeschützte Dateien sein (z.B. AES256 verschlüsselte ZIP Archive).
2. Für den regelmäßigen Wechsel von Passwörtern wird bevorzugt ein automatisiertes Verfahren eingesetzt. Dabei sollten die Nutzer des automatisierten Verfahrens im Vorfeld ein Masterpasswort erhalten, welches beim Wechsel zur Authentisierung des Nutzers dienen soll. Dieses Passwort erlaubt nur den Wechsel und keinen Zugang. Es ist ebenfalls geheim zu halten. Wenn technisch umsetzbar, kann auch ein sicheres TAN-Verfahren (z.B. SMS-TAN) eingesetzt werden.
3. Besteht die Möglichkeit Anwendungssoftware zu konfigurieren, sind die für die Passwortsicherheit aufgestellten Vorgaben umzusetzen, so dass Benutzer nur Passwörter vergeben können, die den folgenden Kriterien genügen und es sind die nachfolgend genannten Sicherheitsoptionen zu aktivieren:
   - Mindestlänge von 8 Zeichen. Bei höherem Schutzbedarf ist die Mindestanzahl an Zeichen zu erhöhen (12 Zeichen und höher).
   - Zeichenmischung von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen um leicht zu erratende Passwörter zu vermeiden.
   - Protokollierung von Fehlversuchen bei der Passworteingabe, um Angriffe und versuchten Missbrauch zu erkennen. Nach mehrmaliger fehlerhafter Passworteingabe (z.B. 5 Versuche) muss die Benutzerkennung gesperrt werden und es muss eine automatisierte Meldung an die Administratoren erfolgen. Alternativ kann auch eine ausreichende Zeitverzögerung zwischen den Eingabeversuchen festgelegt werden.
   - Nach der vorgegebenen Frist (z.B. 180 Tage) wird ein Passwortwechsel erzwungen.
   - Neu erstellte Benutzerkennungen, die länger als 30 Tage nicht aktiviert wurden, werden überprüft und bei Bedarf gesperrt.
   - Passwörter dürfen während der Eingabe nicht in Klartext angezeigt werden.
   - Passwörter müssen einwegverschlüsselt gespeichert werden.
   - Passwörter dürfen in Netzwerken nur verschlüsselt übertragen werden.
   - Bei öffentlich zugänglichen Einrichtungen sind geeignete Maßnahmen zur Abwehr von Brute-Force-Angriffen zum Erraten von Passwörtern zu treffen.
4. Bei der Auswahl von IT-Systemen und Anwendungsprogrammen sind die vorher genannten Mechanismen im Lastenheft als „Muss-Funktion“ aufzuführen. Sofern dies (z.B. aus betriebswirtschaftlichen Gründen) nicht möglich ist, muss eine geeignete Zusatz-Software eingesetzt werden.
5. Fall technische Authentifizierungsmedien zur Passworteingabe eingesetzt werden (z.B. Magnetkarte, Chipkarte, RFID, …), müssen diese so verwahrt werden, dass die Benutzung durch Unbefugte ausgeschlossen ist. Soweit erforderlich werden, abhängig vom Schutzbedarf, besondere Regelungen getroffen.

Verantwortlichkeit

Die Verantwortung für die Umsetzung und Einhaltung der Passwortrichtlinie liegt bei der Unternehmensleitung. Diese überträgt die Aufgaben der operativen Umsetzung der Passwortrichtlinie und die Kontrolle über deren Einhaltung an den Datenschutzbeauftragten.
Die Einhaltung der Passwortrichtlinie wird durch die jeweiligen Vorgesetzten kontrolliert und ist durch Maßnahmen im Rahmen der Dienstaufsicht sicherzustellen. Die Beschäftigten sind mindestens einmal jährlich, oder bei wesentlichen Änderungen der Passwortvorgaben, über den Inhalt dieser Richtlinie zu informieren.

Grundlage der Passwortrichtlinie

Die Grundlage der Umsetzung dieser Passwortrichtlinie ist das Datenschutzkonzept. Diese Richtlinie orientiert sich an den Vorgaben der Datenschutz-Grundverordnung (DSGVO), am Bundesdatenschutzgesetzt (BDSG neu) und am Grundschutzstandard des Bundesamtes für Informationssicherheit (BSI). Prozessverantwortlicher ist der Verantwortliche für den Datenschutz Mustermann.

Inkrafttreten

Diese Richtlinie tritt am XX.XX.20XX in Kraft.

Hinweise zur Nutzung des Dokumentes:

Diese Vorlage für eine Passwortrichtlinie soll nur einen ausführlichen Leitfaden zur Unterstützung eines DSGVO konformen Vorgehens darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit der Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.
Jeder Käufer dieses Produktes ist verpflichtet seine individuellen Ergänzungen und Anpassungen vorzunehmen und die angegebenen Formulierungen für seinen Fall zu prüfen und ggf. zu ändern.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.
8. Das Dokument ist im Kompatibilitätsmodus (*.doc) zu vorherigen Office-Versionen gespeichert. In der Leiste „Datei“, können Sie das Dokument durch Betätigen der Schaltfläche „Konvertieren“ in das aktuelle Format *.docx umspeichern.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.