[Logo der Organisation]

[Name der Organisation]

Commented [EU GDPR1]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

# KENNWORT-RICHTLINIE

Commented [EU GDPR2]: Diese Richtlinie muss nicht als separates Dokument geführt werden, falls die selben Regelungen durch die IT-Sicherheitspolitik und Zugangssteuerungsrichtlinie festgelegt sind.

| | |
|---|---|
| Code: | |
| Version: | |
| Datum der Version: | |
| Erstellt durch: | |
| Genehmigt durch: | |
| Vertraulichkeitsstufe: | |

Commented [EU GDPR3]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

## Änderungs-Historie

| Datum | Version | Erstellt durch | Beschreibung der Änderung |
|---|---|---|---|
| TT.MM.JJJJ | 0.1 | EUGDPRAcademy | Erster Entwurf des Dokuments |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Inhaltsverzeichnis

1. **ZWECK, ANWENDUNGSBEREICH UND ANWENDER** ..... **3**
2. **REFERENZDOKUMENTE** ..... **3**
3. **PFLICHTEN DER ANWENDER** ..... **3**
4. **VERWALTUNG VON BENUTZER-KENNWORTEN** ..... **4**
5. **GÜLTIGKEIT UND DOKUMENTEN-HANDHABUNG** ..... **4**



©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

## 1. Zweck, Anwendungsbereich und Anwender

Der Zweck dieses Dokuments ist, Regeln für das sichere Kennwort-Management und den sicheren Gebrauch von Kennworten festzulegen.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS) und für alle Verarbeitungstätigkeiten von personenbezogenen Daten.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation].

## 2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
- EU DSGVO Artikel 32
- Informationssicherheitspolitik
- Erklärung zur Akzeptanz der ISMS-Dokumente

## 3. Pflichten der Anwender

**Commented [EU GDPR4]:** Diesen Punkt löschen, falls die Regeln bereits in der IT-Sicherheitspolitik festgelegt sind.

Die Anwender müssen bei der Auswahl und Benutzung von Kennworten bewährte sichere Verfahren anwenden:

**Commented [EU GDPR5]:** Diese Regelungen entsprechend der festgestellten Risiken anpassen.

- Kennworte dürfen gegenüber anderen Personen nicht offengelegt werden; dies gilt auch für Geschäftsführung oder Systemadministratoren
- Kennworte dürfen nicht aufgeschrieben werden, außer [Stellenbezeichnung] hat hierfür eine sichere Methode zugelassen
- [illegible]
- [illegible]
- Sichere Kennworte müssen folgendermaßen gewählt werden:
  - Länge von mindestens zwölf (12) Zeichen
  - Benutzung mindestens einer Ziffer
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]



©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

- Kennworte müssen alle 3 Monate geändert werden
- Das Kennwort muss beim erstmaligen Anmelden an einem System geändert werden
- [illegible]
- [illegible]

## 4. Verwaltung von Benutzer-Kennworten

Bei der Bereitstellung und Benutzung von Nutzer-Kennworten müssen folgende Regelungen befolgt werden:

- Mit Unterzeichnung der Annahmeerklärung der ISMS-Dokumente akzeptiert der Nutzer auch die Pflicht zur vertraulichen Behandlung von Kennworten, wie in diesem Dokument vorgeschrieben
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- Das Kennwortmanagement-System muss den Nutzer dazu zwingen, sichere Kennworte zu wählen
- Das Kennwortmanagement-System muss die Nutzer dazu zwingen, ihre Kennworte vierteljährlich zu ändern
- [illegible]
- [illegible]
- Das Kennwort darf während der Anmeldung nicht offen einsehbar sein
- Falls ein Nutzer dreimal in Folge ein falsches Kennwort eingibt, muss das System das betreffende Benutzerkonto sperren
- [illegible]
- [illegible]

**Commented [EU GDPR6]:** Diesen Punkt löschen, falls bereits in der Zugangssteuerungsrichtlinie geregelt.

**Commented [EU GDPR7]:** Diese Regeln an die festgestellten Risiken und an System-Funktionalitäten anpassen.

**Commented [EU GDPR8]:** Unterschiedliche Regeln können für Administrator- und Benutzer-Passworte festgelegt werden.

**Commented [EU GDPR9]:** Hierzu können weitere Details angegeben werden.

**Commented [EU GDPR10]:** z.B. durch E-Mail Versand einer Anweisung an den Benutzer.

**Commented [EU GDPR11]:** z.B. durch Anmeldung am System innerhalb einer bestimmten Zeitspanne, usw.

## 5. Gültigkeit und Dokumenten-Handhabung



©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.

Dieses Dokument ist gültig ab [Datum]

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

**Commented [EU GDPR12]:** Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- Anzahl von Vorfällen in Zusammenhang mit dem Missbrauch von Kennworten durch unberechtigte Personen
- Anzahl von Vorfällen in Zusammenhang mit unsachgemäßem Umgang mit Kennworten

[Stellenbezeichnung]
[Name]

_____

[Unterschrift]

**Commented [EU GDPR13]:** Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.



©2017 Diese Vorlage kann von Kunden von Advisera Expert Solutions Ltd. www.advisera.com gemäß der Lizenzvereinbarung verwendet werden.