[Logo der Organisation]

[Name der Organisation]

KENNWORT-RICHTLINIE

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

Commented [27A1]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A2]: Diese Richtlinie muss nicht als separates Dokument geführt werden, falls die selben Regelungen durch die IT-Sicherheitspolitik und in der Zugangssteuerungsrichtlinie festgelegt sind.

Commented [27A3]: 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.

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
	0.1	27001Academy	Erster Entwurf des Dokuments

Inhaltsverzeichnis

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), d.h. für alle Arbeitsplätze und Systeme innerhalb des ISMS Anwendungsbereiches.

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
- Informationssicherheitspolitik
- Erklärung zur Akzeptanz der ISMS-Dokumente

3. Pflichten der Anwender

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

- [illegible]
- [illegible] sichere Methode zugelassen
- Vom Anwender erstellte Kennworte dürfen auf keinem Weg verbreitet werden (mündlich, [illegible]
- [illegible] gemeldet werden
- [illegible]
  - Länge von mindestens zwölf (12) Zeichen
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible] Name von Familienmitgliedern, etc.)
  - die letzten drei Kennworte dürfen nicht wiederverwendet werden

Commented [27A4]: Diesen Punkt löschen, falls die Regeln bereits in der IT-Sicherheitspolitik festgelegt sind.

Commented [27A5]: Diese Regelungen entsprechend der festgestellten Risiken anpassen.

- Kennworte müssen alle 3 Monate geändert werden
- [illegible]
- [illegible]
- [illegible]

4. Verwaltung von Benutzer-Kennworten

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

- [illegible] vorgeschrieben
- Jeder Nutzer darf nur den ihm/ihr individuell zugewiesenen Benutzernamen benutzen
- [illegible]
- [illegible] festgelegt, einzigartig und sicher sein
- Temporäre Kennworte müssen dem Nutzer auf eine sichere Weise kommuniziert werden
- [illegible]
- Das Kennwortmanagement-System muss den Nutzer dazu zwingen, sichere Kennworte zu wählen
- [illegible]
- [illegible] Identität des Nutzers durch [hier angeben wie] feststellen
- Der Nutzer muss den Empfang des Kennworts durch [hier angeben wie] bestätigen
- [illegible]
- [illegible] betreffende Benutzerkonto sperren
- [illegible]
- [illegible] Anwendung gespeichert werden

5. Gültigkeit und Dokumenten-Handhabung

Commented [27A6]: Diesen Punkt löschen, falls bereits in der Zugangssteuerungsrichtlinie geregelt.

Commented [27A7]: Diese Regeln an die festgestellten Risiken und an System-Funktionalitäten anpassen.

Commented [27A8]: Unterschiedliche Regeln können für Administrator- und Benutzer-Passworte festgelegt werden.

Commented [27A9]: Hierzu können weitere Details angegeben werden.

Commented [27A10]: z.B. durch E-Mail Versand einer Anweisung an den Benutzer.

Commented [27A11]: z.B. durch Anmeldung am System innerhalb einer bestimmten Zeitspanne, usw.

Dieses Dokument ist gültig ab [Datum]

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

Commented [27A12]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A13]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.