Richtlinie Vorgaben für Kennwörter

Version:	*1.0*
Datum:	*30.01.2023*
Klassifizierung:	***NICHT-ÖFFENTLICH***
Status:	*in Arbeit / vorgelegt **/ freigegeben***
Autor:	*Robert Hellwig*
Ablage:	*SharePoint CISO Stabsstelle Informationssicherheit und Datenschutz*

Verteiler:		
	Alle	alle Mitglieder, Angehörige und Gäste der Universität Siegen
cc:	*Kontraktoren*	Externe, die Systeme, Dienste oder Prozesse der Universität Siegen zur Informationsverarbeitung nutzen und insbesondere alle, die Informationen im Auftrag der Universität Siegen verarbeiten.

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	30.01.2023	Robert Hellwig	freigegeben

Definitionen, Abkürzungen, Verweise

Begriff	Definition
Authentisierung	Nachweisen einer Identität
BDSG	Bundesdatenschutzgesetz
CISO	Chief Information Security Officer
DSB	Datenschutzbeauftragter
EU-DSGVO	Datenschutzgrundverordnung der Europäischen Union
ISMT	Informationssicherheitsmanagement-Team
ISO	International Organization for Standardization
Kennwort/Passwort	Geheime Zeichenfolge, die zur Identifikation im Rahmen der Zugangs- und Zugriffskontrolle genutzt wird. Kennwort = Passwort
ZIMT	Zentrum für Informations- und Medientechnologie
2FA/MFA	Zwei-Faktor-Authentisierung/Mehr-Faktor-Authentisierung: Identitätsnachweis eines Nutzers mittels einer Kombination mindestens zweier unterschiedlicher und insbesondere unabhängiger Komponenten

Abstimmungstabelle

Empfänger	Organisation	RACI	
Rektor	Universität Siegen	A	
Kanzler	Universität Siegen	A	
CISO	Universität Siegen	R	
DSB	Universität Siegen	C	
Bereichs-ISBs	Universität Siegen	C	
Leitung ZIMT	Universität Siegen	C	
Alle	Universität Siegen / Externe	I	
Kontraktoren	Externe	I	

RACI Legende: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed

Tabelle 1: RACI Abstimmungstabelle[1]

Verbundene Dokumente

Stammpfad:

Dokumentenname	Ablageort
EU-DSGVO (Gültig ab 25. Mai 2018)	https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.html
BDSG (gültig ab 25. Mai 2018)	https://www.gesetze-im-internet.de/bdsg_2018/
ISO/IEC 27001	https://www.iso.org/isoiec-27001-information-security.html

[1] **Responsible** – verantwortlich (**Durchführungsverantwortung**), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (durch Andere) gibt oder die die Aktivität selbst durchführt.
Accountable – rechenschaftspflichtig (**Kostenverantwortung**), verantwortlich im Sinne von „genehmigen", „billigen" oder „unterschreiben". Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.
Consulted – konsultiert (**Fachverantwortung**). Eine Person, deren Rat eingeholt wird. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
Informed – zu informieren (Informationsrecht)

Geltungsbereich

Diese Kennwortlinie ersetzt alle bisherigen bestehenden Richtlinien in allen Bereichen der Universität Siegen und ist verbindlich für alle internen und externen Systeme, bei denen ein Account der Universität genutzt wird. Mit „Account der Universität“ sind sowohl die dienstlichen E-Mail-Adressen (enden auf uni-siegen.de) als auch die Benutzerkennungen des ZIMT-Kontos (zwei Buchstaben, drei Ziffern oder zwei Buchstaben, 6 Ziffern, ggf. gefolgt von @uni-siegen.de) gemeint.

Diese Regelungen gelten für alle Mitarbeitenden, Studierenden und Gäste der Universität Siegen sowie für alle weiteren Nutzenden von E-Mail-Adressen, die auf „uni-siegen.de“ enden.

Diese Richtlinie regelt die Gestaltung von und den Umgang mit Kennwörtern, die zur Authentisierung berechtigter Benutzer eingesetzt werden.

Für Kennwörter von Konten mit administrativen Rechten gilt eine gesonderte Richtlinie.

Sie ist im Rahmen der technischen Möglichkeiten auf alle IT-Systeme und Telekommunikationssysteme anzuwenden, deren Ressourcen und Daten durch Kennwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden sollen.

Anforderungen an Kennwörter

Das Kennwort muss folgende Voraussetzungen erfüllen:

- Das Kennwort muss eine **Mindestlänge** von **12 Zeichen** haben.
- Das Kennwort muss Zeichen aus **allen drei** folgenden **Kategorien** enthalten:
  - **Kleinbuchstaben** aus dem 26-buchstabigen Alphabet**,**
  - **Großbuchstaben** aus dem 26-buchstabigen Alphabet**,**
  - **Ziffern**.
- Umlaute (ä, Ä, ö, Ö, ü, Ü) oder des ß sowie anderen landes- bzw. sprachspezifischen Buchstaben (z.B. mit Akzenten, Trema, Häkchen [Háček] etc.) bitte nicht verwenden.
- **Sonderzeichen** sind zu **vermeiden** (Beispiele für Sonderzeichen: ~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; " ' < > , . ? /).

- Der **Benutzername** darf **nicht Teil** des Kennwortes sein.

Wo immer es technisch möglich ist, wird die Einhaltung der o.g. Anforderungen seitens der Universität Siegen technisch unterstützt. Unabhängig davon sind diese Vorgaben auch dann einzuhalten, wenn das jeweilige System schwächere Kennwörter zulässt, insbesondere bezüglich der Kennwortlänge.

Umgang mit Kennwörtern

Zusätzlich zu den o.g. Anforderungen sind folgende Vorgehensweisen sicherzustellen:

- Es soll keine regelmäßige Änderung des Kennwortes erfolgen. Eine größtmögliche Länge, optimalerweise über die vorgenannten Mindestanforderungen hinaus, bietet nach aktuellem Stand der Erkenntnisse den besten Schutz.

- Beim Verdacht der Kompromittierung eines Kennworts muss umgehend eine Änderung erfolgen. Das neue Kennwort darf nicht dem bisherigen entsprechen, selbst, wenn das jeweilige System dies zulässt.

- Für jedes System muss ein unterschiedliches Kennwort vergeben werden. Die mehrmalige Verwendung des gleichen Kennwortes soll unbedingt vermieden werden.

- Die Benutzerkennung des ZIMT-Kontos (zwei Buchstaben, drei Ziffern oder zwei Buchstaben, sechs Ziffern, ggf. gefolgt von @uni-siegen.de) darf nur innerhalb der Universität Siegen für vom ZIMT bereitgestellte Systeme genutzt werden.

- Zur Verbesserung der Sicherheit und wo es technisch möglich ist, soll eine Zwei- bzw. Mehr-Faktor-Authentisierung (2FA oder MFA) genutzt werden.

- Das Kennwort darf nur dem jeweiligen autorisierten Benutzer bekannt sein.

- Notierte Kennwörter sind zwingend unter Verschluss aufzubewahren und müssen geheim gehalten werden. Auch die Nutzung eines Passwortmanagers erfüllt diese Bedingung, sofern die o.g. Anforderungen an das Kennwort eingehalten werden.

- Die Eingabe des Kennwortes muss immer unbeobachtet stattfinden.

- Kennwörter dürfen nicht leicht zu erraten sein. Vor- und Familiennamen oder Geburtstage sowie Wörter, die in einem Lexikon nachgeschlagen werden können, sind beispielsweise nicht zur Bildung von Kennwörtern geeignet.

- Es dürfen niemals Trivialkennwörter verwendet werden (z. B. 123456789012, Kennwort1234, ABCDEFGHIJKL, QWERTZUIOPAS oder andere nebeneinanderliegende Tasten).

- Sofern Gruppenkennwörter zwingend erforderlich sind, gilt: Gruppenkennwörter sind umgehend zu ändern, wenn die Zusammensetzung der Gruppe sich verändert. Gleiches gilt, wenn Gruppenkennwörter unautorisierten Personen bekannt geworden sind oder ein entsprechender Verdacht besteht.

- Voreingestellte Kennwörter bzw. von der jeweiligen Einrichtung vergebene Kennwörter müssen umgehend durch individuelle Kennwörter ersetzt werden.

- Alle IT-Systeme sollten zum Schutz der Nutzung durch unbefugte Personen mit einem kennwortunterstützten Bildschirmschoner ausgestattet sein. Die automatische Aktivierung soll aktiviert sein.

Sollte ein (externes) System abweichende Kennwortbedingungen oder -vorgehensweisen anfordern, so ist immer die bestmögliche zu nutzen. I.d.R. ist die in dieser Richtlinie geforderte Kennwortlänge einhaltbar, selbst, wenn das System z.B. nur 8 Zeichen als Mindestlänge erwartet. Sollten regelmäßige Änderungen gefordert sein, so ist das längst mögliche Intervall zu wählen.

Diese Richtlinie tritt durch Veröffentlichung im Intranet in Kraft.

Siegen, den 30. Januar 2023

_____

Robert Hellwig
Chief Information Security Officer (CISO)