KISTERS Passwortrichtlinie

Identitätsmanagement und Authentisierung

v.4.1, 2025-07-29

Verantwortlich:
KISTERS CISO

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Ziele

Der Zugang zu IT-Systemen und Anwendungen und der Zugriff auf die darin verarbeiteten Daten wird über eine personenbezogene Authentifizierung gesteuert. Für die Authentifizierung werden eine eindeutige Kennung des Benutzers (Benutzer- oder Kontoname) sowie ein oder mehrere Berechtigungsnachweise („Credentials“), also Merkmale oder Faktoren benötigt, mit denen die digitale Identität eines Nutzers nachgewiesen werden kann. Zu diesen Merkmalen gehören unter anderem Passwörter, PINs, biometrische Daten oder personenbezogene Geheimnisse. Diese Merkmale bzw. Faktoren müssen besonders vor unbefugtem Zugriff geschützt werden, um die missbräuchliche Nutzung von Nutzerkonten und den zugehörigen Rechten durch unautorisierte Dritte zu verhindern.
Neben der Authentisierung von Nutzern werden Passwörter auch ohne explizite Benutzerangabe verwendet, z.B. für den Zugriffsschutz von Dokumenten, Verschlüsselung von Daten, Zugriff auf individuelle Programme o.ä.
Die in dieser Richtlinie enthaltenen verbindlichen Regelungen gelten allgemein für den Umgang mit Passwörtern und anderen Authentisierungsmitteln.

1.2 Anwendungsbereich

Diese Richtlinie für den Umgang mit Passwörtern gilt für die gesamte KISTERS Gruppe sowie externe Dritte, die Authentisierungsinformationen für den Zugang zu KISTERS IT-Systemen oder den Zugriff auf KISTERS Daten benötigen.
Diese Richtlinie ist Bestandteil der „KISTERS Informationssicherheitsrichtlinie“ [1]. Geltungsbereich, Verbindlichkeit, Terminologie, Ansprechpartner und weitere Informationen gelten entsprechend dem Hauptdokument.

1.3 Rollen, Verantwortlichkeiten und Abhängigkeiten

	ISMT (1)	IT Administration	Systemverantwortliche (1)	Mitarbeiter	Externe Nutzer
Definition Passwortrichtlinien	A/R	I	I	I	I
Bereitstellung Passwortmanagementtools	A	R		I	
Konfiguration IT-Systeme (2)	C	C	A/R	I	I

(1): Wie in der „KISTERS Information Security Organization“ definiert [2].
(2): Soweit von den Systemen die Konfiguration und/oder Überprüfung der Passwortrichtlinien unterstützt wird.

1.4 Anwendbare rechtliche und regulatorische Anforderungen

Die Erstellung einer Richtlinie für Passwörter und andere Autorisierungsinformationen ist eine Grundvoraussetzung für die Einhaltung von ISO 27001, SOC 2, BSI C5 und anderen Informationssicherheitsstandards [3]. In individuellen Verträgen mit Kunden hat sich KISTERS verpflichtet, die Einhaltung eines oder mehrerer dieser Sicherheitsstandards oder gleichwertiger individueller Kundenanforderungen zu gewährleisten und aufrechtzuerhalten.
Die Vorgaben dieser Richtlinie orientieren sich an anerkannten Standards zur Informationssicherheit [4], [5], [6], daher wurde keine gesonderte Risikobetrachtung durchgeführt.

2 Generelle Vorgaben

[INFO] Viele IT-Systeme, Cloud-Dienste und Applikationen verlangen mindestens einen eindeutigen Benutzernamen und ein Passwort, unterstützen aber die optionale Nutzung von weiteren Faktoren für die Authentifizierung. Generell werden folgende Faktoren zur Authentisierung unterschieden:

- Wissensfaktor (was man weiß)
    - Passwort, Passphrase, PIN („Personal Identification Number“), etc.
- Besitzfaktor (was man besitzt)
    - Authenticator-App auf Smartphone, gerätegebundene Telefonnummer, Chipkarte, Hardware-Token, TAN-/OTP-Generator („Transaction Authentication Number“ / „One Time Password“), TAN-Liste, Personalausweis mit Online-Ausweisfunktion, etc.,
- Inhärenzfaktor (was man ist)
    - Fingerabdruck, Irisabbild, Gesichtsabbild, Stimme, andere biometrische Daten.

Grundsätzlich gilt:
Soweit technisch möglich MÜSSEN immer mindestens zwei Faktoren für die Authentifizierung von Nutzern verwendet werden.

Im Folgenden werden die spezifischen Vorgaben für die Nutzung von Wissensfaktoren (Passwörter, PINs) und Besitzfaktoren (Software-, Hardware-Token) spezifiziert.

3 Passwörter

[INFO] Ein Passwort, oder wenn es sich um einen numerischen Wert handelt, eine PIN, ist ein geheimer Datenwert, der Nutzer den Zugang zu IT-Systemen oder Zugriff auf Informationen ermöglicht. Ein Passwort gilt als kompromittiert, wenn unberechtigte Dritte das Passwort in Erfahrung gebracht haben. Ein System gilt kompromittiert, wenn unberechtigte Dritte Zugang zu dem System und/oder Zugriff auf die Information erhalten haben. Das System ist nicht mehr vertrauenswürdig, da möglicherweise alle Daten und Programme manipuliert und alle Informationen, die auf dem System gespeichert oder verarbeitet worden sind, an unberechtigte Dritte weitergegeben wurden.

3.1 Vertraulichkeit und Nutzung

Für den Umgang mit Passwörtern sind die folgenden besonderen Regeln einzuhalten:

- Passwörter MÜSSEN geheim gehalten werden und DÜRFEN NICHT offensichtlich oder einfach zugreifbar sein (z.B. Zettel unter der Tastatur, unverschlüsselte Datei auf dem Rechner o.ä.).
- Passwörter DÜRFEN NICHT über unsichere Kommunikationsmittel (unverschlüsselte E-Mail, Chats, Messenger, etc.) übermittelt werden.
- Passwörter DÜRFEN NICHT in Datenbanken, Dateiablagen oder Foren abgelegt werden, die nicht-autorisierten Personen den Zugriff auf die Passwörter ermöglichen (Jira, Confluence, SITE, Fileserver, etc.)
- Für unterschiedliche Anwendungen MÜSSEN immer unterschiedliche Passwörter verwendet werden. Damit bleibt eine mögliche Kompromittierung eines Passworts auf die betroffene Anwendung beschränkt. Ausgenommen davon sind Anwendungen, die auf eine gemeinsame Nutzerverwaltung zurückgreifen und daher ein gemeinsames nutzerspezifisches Passwort verlangen.
  [INFO] KISTERS intern werden unter anderem die Anmeldungen eines Nutzers am Arbeitsplatzrechner, am VPN-Zugang, an Microsoft Outlook und Teams, an Confluence und Jira über die Nutzerverwaltung des zentralen Microsoft Active Directory durchgeführt und verwenden dasselbe nutzerspezifische Passwort.
- Insbesondere DÜRFEN die für Firmenanwendungen verwendeten Passwörter NICHT zur Anmeldung an externen Anwendungen und Systemen (externe E-Mail-Accounts, Service-Accounts, Foren, TeamViewer, Skype, etc.) verwendet werden, unabhängig davon, ob diese privat oder dienstlich genutzt werden.
- Passwörter für nicht-persönliche Benutzerkonten (wie z.B. Firmen-, Gruppen-, Administrator-, Test- oder Wartungskonten), Anwendungen oder Dateien DÜRFEN NUR an Benutzer weitergegeben werden, die zum Zugriff auf die betroffenen Systeme und Informationen autorisiert sind.

3.2 Eigenschaften von Passwörtern

[INFO] Passwörter sollen „schwer zu knacken, aber leicht zu behalten“ sein. Um das Herausfinden von Passwörtern durch Erraten aufgrund von Wissen über die Person des Nutzers oder durch das softwaregestützte methodische Ausprobieren von Passwörtern („brute-force attack“) zu erschweren, werden folgende allgemeine Anforderungen an Passwörter gestellt:

- Passwörter MÜSSEN mindestens **12** Zeichen lang sein, je länger desto besser.
- Passwörter für administrative Benutzerkonten oder für Information mit besonderem Schutzbedarf (z.B. Password Stores) MÜSSEN mindestens **14** Zeichen lang sein, je länger desto besser.
- Passwörter MÜSSEN mindestens 3 der folgenden Zeichentypen beinhalten:
  - Großbuchstaben
  - Kleinbuchstaben
  - Zahlen
  - Sonderzeichen: Im Allgemeinen werden mindestens die folgenden Zeichen unterstützt, je nach Applikation kann es jedoch spezifische Randbedingungen und Einschränkungen geben:
    `~!@#$%^_-+` () [] : . ?`
- Passwörter DÜRFEN NICHT leicht zu erraten oder durch „brute-force attacks“ herauszufinden sein.
  Die folgenden Beispiele werden als unsicher angesehen und DÜRFEN NICHT verwendet werden:

- der eigene Name, der Nutzername, das Login oder die E-Mail-Adresse
- Namen von Familienangehörigen (Lebensgefährte, Kinder, Eltern, …)
- Name von Haustieren
- Namen von Freunden, Kollegen oder Chefs
- Namen von bekannten Künstlern, Politikern etc.
- Ortsnamen (Straßen-, Städte-, Ländernamen o.ä.)
- überhaupt Namen
- Telefonnummern
- Geburtstage
- der für die Anmeldung am IT-System verwendete Benutzername
- der Name des Betriebssystems oder der Anwendung
- ein Wort aus einem Wörterbuch oder einfache Kombinationen davon, z.B.: „`TeamPasswort`“, „`GutesTeamPasswort`“, u.ä.)
- Wörterbuch-Wörter, bei denen Buchstaben durch ähnlich aussehende Ziffern oder Sondereichen ersetzt werden („Leet Speech“), z.B. „`TeamPassw0rt`“, „`Z1tr0nen$aft`“, u.ä.)
- einfache oder bekannte Zeichenfolgen wie `abcd`, `12345`, `qwertz`, `0815`, `4711` (auch nicht mit Großbuchstaben)
- alle obengenannten Varianten rückwärts geschrieben oder nur von einer Zahl oder einem Sonderzeichen gefolgt

- Folgende Möglichkeiten zur Auswahl von sichereren Passwörtern SOLLEN angewendet werden:
  - Generierung mithilfe eines Passwort-Generators
  - Längere Zeichenketten aus einer Vielzahl von Wörtern, sogenannte „Pass-Phrases“, jedoch keine allgemein bekannten Aussprüche, Redewendungen, Zitate, Liedzeilen oder ähnliches, sondern selbst ausgedachte Phrasen, z.B.
    - „`MeinAutohat2Tueren+1Motor+4Raeder`“
    - „`KochenIstSuper-TellerEherRuhigSo`“
  - Verwendung einer Pass-Phrase, aus der ein Passwort durch Abkürzung oder symbolische Ersetzung gebildet wird (auch hier keine bekannten Phrasen, s.o.), z.B.
    - „Bei KISTERS macht die Arbeit mehr Spaß als sonstwo“ → „`@KSTRSmdA+Sas`“
    - „Wer Rom an einem Tag erbaut – der hat uns den Akkord versaut!“ → „`?Ra1Te-dhudAv!`“
    - “My jersey number when I played competitive soccer was 27!” → “Mj#wIpcsw27!“

Vor der Auswahl eines Passworts für eine Anwendung oder ein IT-System MUSS geprüft werden, ob es zusätzliche Anforderungen oder spezielle Einschränkungen bezüglich der Passwort-Auswahl gibt. Im Falle von Einschränkungen MÜSSEN die o.g. Vorgaben bestmöglich umgesetzt werden.

3.3 Änderung von Passwörtern

[INFO] In bestimmten Situationen können oder müssen Passwörter geändert werden. Es gelten die folgenden Regelungen:

- Passwörter KÖNNEN regelmäßig geändert werden.
- Die Häufigkeit eines regelmäßigen Passwortwechsels KANN durch technische oder besondere organisatorische Maßnahmen vorgeschrieben werden. Wenn dies nicht der Fall ist, dann KANN der Benutzer selbst über den Passwortwechsel entscheiden.
- Ein Passwort MUSS in jedem Fall geändert werden, wenn das Passwort oder das damit zugängliche System kompromittiert worden ist oder der Verdacht einer Kompromittierung besteht.
- Voreingestellte, initial vom Systemverantwortlichen vergebene Passwörter und Default-Passwörter von Anwendungen und IT-Systemen MÜSSEN von den Nutzern bei der ersten Anmeldung geändert werden, sofern eine Passwortänderung durch die Nutzer technisch möglich ist und diese die notwendige Berechtigung haben.
- Passwörter für nicht-persönliche Benutzerkonten (wie z.B. Firmen-, Gruppen-, Administrator--, Test- oder Wartungskonten) MÜSSEN zwingend geändert werden, wenn ein autorisierter Benutzer von der Nutzung des Systems oder der Daten ausgeschlossen wird, z.B. beim Austritt aus dem Unternehmen oder Wechsel des Aufgabenbereichs.
- Bei der Änderung von Passwörtern MUSS sich das neue Passwort deutlich vom vorherigen unterscheiden, um ein Erraten aufgrund von einfachen Mustern auszuschließen (z.B. „`Passwort2019`“ → „`Passwort2020`“).
- Einmal gewählte Passwörter DÜRFEN NUR nach mindestens 24 Passwortänderungen wieder ausgewählt werden.

In jedem Fall MÜSSEN spezifische Anforderungen zum Passwortwechsel von IT-Systemen und Anwendungen beachtet werden.
[INFO] Benutzer werden von den Systemverantwortlichen informiert, falls ein systembedingter oder anlassbezogener Passwortwechsel durch die Systemverantwortlichen vorgenommen wurde.

3.4 Verfügbarkeit von Passwörtern

[INFO] Die Hinterlegung von Passwörtern ist problematisch, da bei Hinterlegung an nicht geschützten Orten oder in nicht geschützten Medien die Autorisierung des Zugriffs nicht gewährleistet werden kann.

- Passwörter für nicht-persönliche Benutzerkonten (wie z.B. Firmen-, Gruppen-, Administrator--, Test- oder Wartungskonten) MÜSSEN immer dem Hauptnutzer bzw. Verantwortlichen für das System und seinem Vertreter bekannt sein.
- Passwörter MÜSSEN bei der IT-Administration hinterlegt werden, wenn es keine andere technische oder organisatorische Lösung gibt, beim Ausfall der verantwortlichen Mitarbeiter den über diese Passwörter abgesicherten Zugriff auf Information oder IT-Systeme durch andere autorisierte Mitarbeiter sicherzustellen.

3.5 Passwörter für Servicekonten auf externen Systemen

[INFO] Für KISTERS Mitarbeiter werden vielfach auf Kunden- oder Partnersystemen Benutzerkonten eingerichtet, um KISTERS eine Nutzung der Systeme oder auch die Wartung und Systemanalyse zu ermöglichen. Unabhängig davon, durch wen diese Konten eingerichtet werden, gelten folgende Regelungen für die auf diesen Systemen genutzten Passwörter:

- Die Passwörter von KISTERS Servicekonten auf IT-Systemen externer Dritter (Kunden, Partner, etc.) MÜSSEN den Passwortrichtlinien des jeweiligen Systembetreibers genügen.

- Falls die Passwortrichtlinien des Systembetreibers in einzelnen Punkten schwächer oder weniger restriktiv sind als die KISTERS Passwortrichtlinien, so MÜSSEN in diesen Punkten die KISTERS Passwortrichtlinien befolgt werden, soweit dies technisch möglich ist.
- Passwörter für Servicekonten DÜRFEN NICHT mehrfach, d.h. für Systeme verschiedener externer Dritter, verwendet werden, um das Risiko einer Folge-Kompromittierung von weiteren Systemen nach einem Sicherheitsvorfall bei einem externen Dritten zu verringern.

4 Personal Identification Numbers (PINs)

[INFO] Mobile Geräte wie Smartphones oder Tablets verwenden in der Regel PINs zur Entsperrung der SIM-Karte (SIM-PIN) nach dem Einschalten des Geräts und zur Entsperrung der Bedienfläche (Display-PIN) nach Inaktivität oder Ruhezustand.
Für PINs MÜSSEN die oben beschriebenen Sicherheitsmaßnahmen wie für Passwörter angewendet werden. Zusätzlich ist zu beachten:

- PINs SOLLEN eine Mindestlänge von 6 Zeichen/Ziffern haben, dabei ist die Auswahl von PINs den Möglichkeiten bzw. Einschränkungen der Geräte anzupassen.
- Sofern ein Gerät unterschiedliche PINs unterstützt (SIM-PIN und Display-PIN), so MÜSSEN diese verschieden sein.

5 Werkzeugunterstützung für den Umgang mit Passwörtern

5.1 Passwort Manager

[INFO] „Passwort Manager“ („Password Stores“) sind Programme, die die sichere Speicherung von Passwörtern ermöglichen und in der Regel auch Passwort-Generatoren beinhalten. Geeignete Softwarelösungen werden von der IT-Administration zur Verfügung gestellt, Information hierzu ist im KISTERS Confluence unter dem Suchbegriff „password manager“ verfügbar.

- Zur Speicherung und Verwaltung von persönlichen Passwörtern und PINs MUSS ein Password Store verwendet werden (z.B. KeePass, KeePass2, KeePassXC), dessen Datenbank lokal gesichert werden SOLL.
- Verschiedene Browser bieten an, Passwörter von besuchten Internetseiten oder Browser-basierten Anwendungen zu speichern. Diese Funktion SOLL NICHT genutzt werden, da die Passwörter leicht durch sogenannte „Password-Stealer“ aus den Browsern ausgelesen werden können. Falls diese Funktion dennoch verwendet wird, dann MÜSSEN die Passwörter im Browser durch ein „Master-Passwort“ gesichert werden, andernfalls MUSS das Speichern von Passwörtern im Browser abgelehnt werden.
- Passwörter für Password Stores und Master-Passwörter MÜSSEN immer mindestens **14** Zeichen haben.
- Passwörter, die zum Zugang auf Kundensysteme (beim Kunden über Fernwartung oder in KISTERScloud) verwendet werden, MÜSSEN im zugangsbeschränkten „Remote Maintenance“- Bereich der „New Customer Care“-Datenbank abgelegt werden.
- Passwörter für gemeinsam genutzte Service-Konten auf externen Systemen oder andere nicht personenbezogene geschäftliche Zugänge MÜSSEN in einem gemeinsamen Password-Store abgelegt werden.

[INFO] Als zentraler Multi-User Password-Store wird Vaultwarden von der IT-Systemadministration bereitgestellt.

5.2 Übertragung von Passwörtern

Für die Übertragung von Passwörtern MUSS ein sicheres Verfahren verwendet werden, das einen Zugriff Unbefugter auf die Passwörter ausschließt. Mögliche Verfahren sind:

- mündliche Weitergabe
  - telefonisch, face-to-face
- schriftliche Weitergabe
  - in einem verschlossenen/versiegelten Briefumschlag mit Vermerk persönlich/vertraulich
- Nutzung eines gemeinsamen, zugangsgesicherten Passwortspeichers
  - NCC, zugangsbeschränkte Confluence-Seiten, Passwort-Manager
- E-Mail
  - Intern: In Outlook als "**Privat**" kennzeichnen
  - Extern: S/MIME Verschlüsselung - nur möglich, wenn ein sowohl Sender als auch Empfänger personenbezogenes S/MIME-Zertifikate ausgetauscht haben
- KISTERS PrivateBin
  - Hier wird das Passwort verschlüsselt und in einer Datenbank abgelegt. Es wird ein Web-Link zum Abruf des Passworts generiert, der dem Empfänger zugestellt wird. Information hierzu ist im KISTERS Confluence unter dem Suchbegriff „PrivateBin“ verfügbar.

6 Security-Token

Die folgenden Security-Token SOLLEN als Besitzfaktoren verwendet werden:

- Hardware-Token
  - Time-based One-Time Password Authenticator (TOTP), z.B. RSA SecurID
  - Yubico Yubikey FIDO2 key
- Software-Token
  - Microsoft Authenticator
  - Google Authenticator (TOTP)
  - Yubico Authenticator (TOTP)
  - FreeOTP (TOTP)

Weitere Security-Token KÖNNEN als Besitzfaktoren durch die IT-Administration freigegeben werden.

6.1 Hardware-Token

Für die Nutzung von Hardware-Token gelten folgende Richtlinien:

- Für dienstliche Zwecke DÜRFEN NUR Hardware-Token verwendet werden, die von der IT-Administration beschafft oder freigegeben wurden.
- Hardware-Token MÜSSEN sicher aufbewahrt und vor Verlust und unbefugtem Zugriff geschützt werden.

- Hardware-Token SOLLEN NICHT zusammen mit anderen Gegenständen (z.B. Firmenausweis) aufbewahrt werden, die unmittelbar eine persönliche Identifizierung und Zuordnung zu KISTERS ermöglichen.
- Der Verlust oder die Entwendung eines Hardware-Tokens MUSS unverzüglich der IT-Administration gemeldet werden, damit eine unbefugte Nutzung durch Sperren des Zugangsmittels ermöglicht wird.

6.2 Software-Token

[INFO] Software-Token bestehen aus einer Software, die in der Regel als App auf einem Smartphone installiert wird und einem vom Identitätsprovider (z.B. Microsoft) für den Nutzer ausgestellten gemeinsamen Geheimnis (Shared Secret), welches beim Identitätsprovider und in der App bzw. auf dem Smartphone gespeichert wird. Auf Basis dieses gemeinsamen Geheimnisses können der Identitätsprovider und die App unabhängig voneinander einen einmaligen Code mit zeitlich beschränkter Gültigkeit generieren, z.B. 6 Zahlen, der bei der Authentifizierung überprüft wird.
[INFO] Gemeinsam haben die unterschiedlichen Software-Token, dass bei der Ausstellung des Tokens das gemeinsame Geheimnis zur App übertragen oder per QR-Code abfotografiert wird. Je nach Verfahren kann das gemeinsame Geheimnis dabei in beliebig viele Apps übertragen werden. Auch kann das gemeinsame Geheimnis möglicherweise nach der Übertragung noch kopiert werden, sofern die App dieses nicht unterbindet.

Aus diesen Gründen MÜSSEN im Umgang mit Software-Token die folgenden Regeln befolgt werden.

- Speicherung von gemeinsamen Geheimnissen
    - Die Speicherung eines gemeinsamen Geheimnisses MUSS verschlüsselt erfolgen. Befindet sich das Software-Token in einer App auf einem Smartphone, so MUSS der Speicher des Smartphones verschlüsselt sein.
    - Der Zugriff auf den verschlüsselten Speicher MUSS entsprechend dieser Richtlinie mit einem sicheren Passwort versehen sein.
    - [INFO] Der Speicher alle aktuellen Mobiltelefone und Tablets ist mit einer „full-disk encryption“ gesichert.
- Backup von Software-Token
    - Auf eine Sicherung (Backup) von Software-Token SOLLTE verzichtet werden.
    - Stattdessen SOLLTE mindestens ein weiteres Security-Token vorhanden sein.
- Übertragung von Software-Token
    - Auf eine Übertragung von Software-Token SOLLTE verzichtet werden.
    - Stattdessen SOLLTE ein neues Software-Token erstellt und das alte Software-Token gelöscht werden.
- Verlust eines Software-Tokens
    - Bei Verlust eines Software-Tokens (z.B. Verlust des Mobiltelefons, auf dem das Software-Token installiert ist) MUSS dieses umgehend beim Identitätsanbieter gelöscht werden.
    - Der Verlust MUSS unverzüglich der IT-Administration gemeldet werden, damit diese Löschung durchgeführt wird.

- Für den Identitätsanbieter Microsoft KANN der Benutzer selbst unter https://mysignins.microsoft.com/security-info die Löschung vornehmen.

7 Meldungen von Sicherheitsereignissen und -vorfällen

Wenn ein Mitarbeiter die Kompromittierung eines Passwortes, eines Security-Tokens oder eines IT-Systems feststellt oder der Verdacht einer Kompromittierung besteht, dann MÜSSEN die Maßnahmen zur Meldung von Sicherheitsvorfällen entsprechend der „KISTERS Informationssicherheitsrichtlinie“ durchgeführt werden. Bei akuten Sicherheitsvorfällen mit potentiell weiterreichenden Konsequenzen für Daten- oder Systemsicherheit MUSS der Mitarbeiter in jedem Fall folgende Personen benachrichtigen:

- die IT-Administration,
- den CISO und den Datenschutzbeauftragten,
- die Verantwortlichen für betroffene IT-Systeme.

8 Referenzen

[1] “KISTERS Informationssicherheits-Richtlinie”, KISTERS ISMS, Confluence
[2] “KISTERS Information Security Organisation”, KISTERS ISMS, Confluence
[3] “KISTERS Information Security Laws and Regulations”, KISTERS ISMS, Confluence
[4] “BSI Grundschutzkompendium, ORP.4: Identitäts- und Berechtigungsmanagement”, Bundesamt für Sicherheit in der Informationstechnik (BSI), Feb. 2023; URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.html (2024-05-06).
[5] “NIST SP 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management”, Technical Report CMU/SEI-2004-HB-003, National Institutes of Standards and Technology (NIST), 2020-03-02; URL: https://pages.nist.gov/800-63-3/sp800-63b.html (2024-05-06).
[6] “OWASP Application Security Verification Standard “, v.4.0.3, OWASP, October 2021, URL: https://owasp.org/www-project-application-security-verification-standard/ (2024-05-06).

9 Dokumenthistorie

Dieses Dokument wird mindestens einmal pro Jahr auf Aktualität geprüft und ggfs. angepasst. Die offizielle Version dieses Dokuments wird online verwaltet. Vor der Verwendung von elektronischen Kopien oder gedruckten Versionen sind diese auf Aktualität zu überprüfen.

Version	Datum	Editor*in	Aktion
4.1	2025-07-29	J. Rade	Anpassung bzgl. der Nutzung von Passwort Managern
4.0	2024-07-19	Jens Weber, H.-J. Schlebusch	Ergänzungen MFA und Security-Token, Anpassung Nutzung Passwort-Manager, Aktualisierung der Referenzen
3.0	2023-03-23	H.-J. Schlebusch	Struktur angepasst an C5 SP-01 Dokumentvorlage; Ergänzungen: Ziele, Anwendungsbereich, Rollen, rechtliche Anforderungen, Referenzen
2.2	2022-07-07	H.-J. Schlebusch	Ergänzungen Pass-Phrase, Anpassung Regelung 2FA

Version	Datum	Editor*in	Aktion
2.1	2020-11-11	H.-J. Schlebusch	Änderungen aufgrund von A/D-LDAP-Konsolidierung und Wechsel zu Outlook
2.0	2020-09-25	H.-J. Schlebusch, B. Kisters	Restrukturiert; Minimale Passwortlänge angepasst an neue Vorgaben; Multifaktor Authentisierung ergänzt
1.5	2020-01-21	H.-J. Schlebusch	Redaktionelle Änderungen, Ergänzung „Jira“
1.4	2018-11-13	H.-J. Schlebusch	Erweiterte Passwortregel für administrative Accounts
1.3	2018-08-01	H.-J. Schlebusch	Überprüfung, keine inhaltliche Änderung notwendig
1.2	2017-11-27	H.-J. Schlebusch	Passwörter für Systeme externer Dritter
1.1	2017-10-19	H.-J. Schlebusch	Werkzeuge für Passwort Management
1.0	2016-10-21	H.-J. Schlebusch	Erstellung durch Auslösung aus KISTERS Informationssicherheitsrichtlinie