heylogin

Leitfaden zur ISMS-Integration

Hinweise und Vorlagen zur Integration von heylogin in das Informationssicherheits-Managementsystem Ihrer Organisation

heylogin GmbH

11. August 2026, Version: v1.0

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck dieses Dokuments

Dieser Leitfaden unterstützt Organisationen, die heylogin einsetzen, bei der Integration in ihr eigenes Informationssicherheits-Managementsystem (ISMS). Er enthält sachliche Zusammenfassungen der Sicherheitseigenschaften von heylogin sowie unmittelbar anpassbare Vorlagentexte für gängige ISMS-Dokumente.

Unabhängig davon, ob Ihr ISMS auf ISO/IEC 27001, TISAX oder einem vergleichbaren Rahmenwerk basiert: Der Einsatz einer Passwortverwaltung muss in mehreren Richtlinienbereichen dokumentiert werden. Dieser Leitfaden bündelt die dafür benötigten Informationen an einer Stelle und stellt Formulierungsvorschläge bereit, die Sie an Ihre Organisation anpassen können.

1.2 Verwendung dieses Leitfadens

Jeder Abschnitt behandelt einen ISMS-Richtlinienbereich, der von der Einführung und Nutzung von heylogin betroffen ist. Die Abschnitte sind wie folgt aufgebaut:

- **Kontext** erläutert, warum der Richtlinienbereich relevant ist und welche ISO 27001-Maßnahmen greifen.
- **Was heylogin bereitstellt** fasst die relevanten Fakten zusammen, basierend auf den Angaben von heylogin, den veröffentlichten Whitepapern und der ISMS-Dokumentation.
- **Vorlagentext** (durch eine Linie am linken Rand gekennzeichnet) enthält Formulierungen, die Sie in Ihre eigenen Richtliniendokumente übernehmen und anpassen können. Platzhalter sind als `[IHR ...]` gekennzeichnet und müssen durch die Angaben Ihrer Organisation ersetzt werden. Bitte beachten Sie, dass die Formulierungen allgemein gehalten sind. Einzelne Begriffe können in Ihrer Organisation abweichen.

1.3 Zur Sicherheitslage von heylogin

Die heylogin GmbH betreibt ein ISMS, das durch den TÜV Rheinland nach **ISO/IEC 27001:2022 zertifiziert** ist (Prüfzeichennummer 9000032416). Der Zertifizierungsumfang umfasst die Entwicklung, den Betrieb und die Vermarktung der Passwortverwaltung heylogin.

Wesentliche Sicherheitseigenschaften des heylogin-Dienstes:

- **Ende-zu-Ende-Verschlüsselung** aller Kundeninhalte (Passwörter, Zugangsdaten, Metadaten). Der heylogin-Server dient ausschließlich als Synchronisationsstelle für verschlüsselte Daten und hat keine technische Möglichkeit, auf Inhaltsdaten zuzugreifen (Zero-Knowledge-Architektur).
- **Hardwaregestützte Zwei-Faktor-Sicherheit by design.** Die Entschlüsselung erfordert sowohl das Gerät des Nutzers (Besitzfaktor) als auch eine biometrische oder PIN-Authentifizierung (Wissens- bzw. biometrischer Faktor). Ein Master-Passwort wird nicht verwendet.
- **Datensouveränität.** Die gesamte Produktivinfrastruktur und alle Backups befinden sich in Deutschland und werden von ISO 27001-zertifizierten Rechenzentrumsbetreibern bereitgestellt.
- **Externe Datenschutzprüfung.** Die datenschutzrechtliche Einordnung wurde von einem unabhängigen externen Datenschutzbeauftragten (Projekt 29 GmbH & Co. KG) geprüft, der die Eignung für den Einsatz in stark regulierten Umgebungen bestätigt.

Weitere Einzelheiten finden Sie in:

- heylogin Security Whitepaper: aktuelle Version in unserem Trust Center
- heylogin Compliance Whitepaper: aktuelle Version in unserem Trust Center
- ISO 27001-Zertifikat: aktuelle Version in unserem Trust Center

2 Lieferantenbewertung

2.1 Kontext

Jedes ISMS erfordert die Bewertung und laufende Überwachung von Lieferanten, die Informationen im Auftrag der Organisation verarbeiten oder speichern. Als Anbieter Ihrer Passwortverwaltung ist heylogin ein Lieferant, der hochsensible Daten (Authentisierungsinformationen) verarbeitet und entsprechend zu bewerten ist.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.5.19 (Informationssicherheit in Lieferantenbeziehungen), A.5.20 (Adressierung der Informationssicherheit in Lieferantenvereinbarungen), A.5.21 (Umgang mit der Informationssicherheit in der IKT-Lieferkette), A.5.22 (Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen)

2.2 Was heylogin bereitstellt

- **Lieferant:** heylogin GmbH, Sophienstraße 40, 38118 Braunschweig, Deutschland
- **Leistung:** Cloudbasierte Passwortverwaltung für Unternehmen
- **Zertifizierung:** ISO/IEC 27001:2022
- **Ort der Datenverarbeitung:** Deutschland (Nürnberg, Falkenstein, Frankfurt)
- **Rechenzentrumsbetreiber:** Hetzner Online GmbH, IONOS SE (beide ISO 27001-zertifiziert)
- **Liste der Unterauftragsverarbeiter:** verfügbar unter heylogin.com/de/avv
- **AVV:** verfügbar unter heylogin.com/de/avv; beidseitige Signatur auf Anfrage über Yousign
- **Architektur:** Zero-Knowledge, Ende-zu-Ende-verschlüsselt; der Anbieter kann nicht auf Inhaltsdaten zugreifen
- **Schwachstellenmeldung:** öffentliche VDP unter heylogin.com/de/schwachstellenmeldung; security@heylogin.com

2.3 Vorlage: Eintrag im Lieferantenverzeichnis

> - **Lieferant:** heylogin GmbH
> - **Leistung:** Passwortverwaltung für Unternehmen (cloudbasiert)
> - **Klassifizierung der verarbeiteten Daten:** vertraulich / hochsensibel (Authentisierungsinformationen)
> - **Vertragliche Grundlage:** `[IHR Verweis auf den Abonnementvertrag]`
> - **AVV:** geschlossen am `[DATUM]`, Version `[VERSION]`
> - **Zertifizierung:** ISO/IEC 27001:2022
> - **Ort der Datenverarbeitung:** Deutschland
> - **Unterauftragsverarbeiter:** verfügbar unter heylogin.com/de/avv; keine außereuropäischen Verarbeiter
> - **Überprüfungsintervall:** `[IHR Prüfzyklus, z. B. jährlich]`
> - **Risikoverantwortlicher:** `[NAME / ROLLE]`

2.4 Vorlage: Lieferantenrisikobewertung

> **Ausfallrisiko:** niedrig.
>
> Die heylogin GmbH ist nach ISO 27001:2022 zertifiziert. Die Architektur des Dienstes umfasst Redundanz über geografisch getrennte Rechenzentren in Deutschland, mit einer nachgewiesenen tatsächlichen Wiederherstellungszeit von unter 2 Stunden und einem Recovery Point Objective von 60 Minuten. Die Client-Anwendungen halten einen lokalen Cache

> vor, sodass Zugangsdaten auch während einer Störung des Dienstes weiter genutzt werden können.
>
> **Auswirkung eines Ausfalls:** `[Bewertung anhand der Abhängigkeit Ihrer Organisation. Zu berücksichtigen: Wie viele Systeme werden über heylogin erreicht? Existiert ein Export- oder Offline-Rückfallverfahren?]`
>
> **Risiko für die Vertraulichkeit der Daten:** niedrig.
>
> Die Zero-Knowledge-Architektur stellt sicher, dass die heylogin GmbH keine technische Möglichkeit hat, auf gespeicherte Zugangsdaten zuzugreifen. Alle Inhaltsdaten werden auf dem Gerät des Nutzers Ende-zu-Ende verschlüsselt, bevor sie an den Server übertragen werden. Selbst bei einer vollständigen Kompromittierung der Infrastruktur des Anbieters können die verschlüsselten Tresore ohne Zugriff auf den Hardware-Sicherheitschip des Nutzers nicht entschlüsselt werden.
>
> **Gesamtrisiko des Lieferanten:** `[Berechnung gemäß Ihrer Methodik]`
>
> **Freigegeben durch:** `[NAME / ROLLE]` am `[DATUM]`

3 Richtlinie zur Zugangssteuerung und Passwortverwaltung

3.1 Kontext

Die Einführung einer zentralen Passwortverwaltung ist eine der wirkungsvollsten Veränderungen der Zugangssteuerung einer Organisation. Ihre Richtlinie zur Zugangssteuerung sollte dokumentieren, welches System eingesetzt wird, wie Zugangsdaten verwaltet werden und welche Regeln für Beschäftigte gelten.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.5.15 (Zugangssteuerung), A.5.16 (Identitätsmanagement), A.5.17 (Authentisierungsinformationen), A.8.02 (Privilegierte Zugangsrechte), A.8.05 (Sichere Authentisierung)

3.2 Was heylogin bereitstellt

- **Zentrale Speicherung von Zugangsdaten** mit Ende-zu-Ende-Verschlüsselung. Zugangsdaten werden in persönlichen Tresoren und geteilten Team-Tresoren organisiert.

- **Automatische Erzeugung starker Passwörter** (Standardlänge 16 Zeichen, konfigurierbar). Die Standard-Passwortrichtlinie folgt den Empfehlungen des CIS Password Policy Guide sowie NIST SP 800-63B.
- **Zwei-Faktor-Sicherheit by design.** Jeder Zugriff auf Zugangsdaten erfordert das authentisierte Gerät des Nutzers (Smartphone mit Biometrie/PIN oder FIDO2-Sicherheitsschlüssel). Dies ist keine optionale Erweiterung, sondern grundlegender Bestandteil der Architektur.
- **Teambasierte Freigabe.** Administratoren können Zugangsdaten Teams zuordnen und steuern, wer Zugriff erhält. Zugriff auf Konten kann auch geteilt werden, ohne das zugrunde liegende Passwort offenzulegen.
- **Audit-Log.** Wesentliche Ereignisse zur Nutzung und Verwaltung von Logins werden protokolliert.
- **Administrative Übersicht ohne Inhaltszugriff.** Administratoren können erkennen, welche Logins existieren und ob diese den Sicherheitsvorgaben entsprechen (z. B. Passwortstärke), können Passwörter jedoch technisch nicht im Klartext einsehen.
- **Automatische Sperrung.** Die Browsererweiterung sperrt sich am Ende des Arbeitstages automatisch.
- **Trennung des privaten Tresors.** Beschäftigte können einen privaten Tresor für private Zugangsdaten nutzen. Administratoren haben darauf keinen technischen Zugriff und keine Einsicht, auch nicht auf Metadaten.

3.3 Vorlage: Richtlinie zur Passwortverwaltung

> **Passwortverwaltung**
>
> `[IHRE ORGANISATION]` setzt **heylogin** als Passwortverwaltung für das Unternehmen ein. Alle Beschäftigten sind verpflichtet, heylogin zur Verwaltung dienstlicher Zugangsdaten zu nutzen. Dies ist keine bloße Empfehlung.
>
> **Anwendungsbereich.** Diese Richtlinie gilt für alle Zugangsdaten, die für den Zugriff auf Systeme, Anwendungen und Dienste im Auftrag von `[IHRE ORGANISATION]` verwendet werden.
>
> **Allgemeine Regeln:**
>
> 1. Alle dienstlichen Zugangsdaten (Benutzernamen, Passwörter, TOTP-Geheimnisse und zugehörige Daten) sind ausschließlich in heylogin zu speichern.
> 2. Zugangsdaten dürfen nicht in anderen Passwortmanagern, in browsereigenen Speichern, in Textdateien, Tabellen oder Ähnlichem gespeichert werden.

3. Zugangsdaten dürfen nicht im Klartext übermittelt werden (z. B. per E-Mail oder Chat). Ist eine Weitergabe erforderlich, erfolgt sie über heylogin-Teams oder extern über die Freigabefunktion von heylogin.

Passworterzeugung:

1. Für alle neuen Konten sowie bei einem Passwortwechsel sind Passwörter mit dem integrierten Generator von heylogin bei einer Standardlänge von 16 Zeichen zu erzeugen.
2. Manuell gewählte Passwörter sind nur zulässig, wenn technische Einschränkungen die Verwendung generierter Passwörter verhindern. In diesen Fällen muss das Passwort mindestens `[IHRE VORGABE]` Zeichen lang sein.

Authentisierung und Entsperren:

1. heylogin darf mit den folgenden Methoden entsperrt werden:

a. Das Smartphone der Beschäftigten, gesichert durch Biometrie oder eine nicht triviale PIN. Dies ist die Standardmethode.
b. Ein FIDO2-Sicherheitsschlüssel mit konfigurierter Nutzerverifikation `[BIOMETRIE ODER NICHT TRIVIALE PIN]`.

2. Geht ein Smartphone oder Sicherheitsschlüssel, der zum Entsperren von heylogin genutzt wird, verloren oder wird gestolen, ist dies **unverzüglich** an `[IHRE IT-ANSPRECHSTELLE / ROLLE]` zu melden. Der Zugriff wird ohne Verzug entzogen.

Geteilte Zugangsdaten:

1. Zugangsdaten, die von mehreren Beschäftigten genutzt werden, sind in heylogin-Teams zu organisieren. Für jedes Team ist eine verantwortliche Person für die Verwaltung der Mitgliedschaften zu benennen *(z. B. Team-Administrator, Teamleitung usw.)*.
2. Der Zugriff auf heylogin-Teams wird nach dem Grundsatz der erforderlichen Nutzung gewährt und `[IHR ZYKLUS, z. B. vierteljährlich]` überprüft.

Ausnahmen:

1. Jede Ausnahme von dieser Richtlinie ist von `[ROLLE, z. B. CISO oder IT-Leitung]` zu genehmigen und zu dokumentieren.

3.4 Vorlage: Richtlinie zur Mehr-Faktor-Authentisierung

> **Mehr-Faktor-Authentisierung**
>
> `[IHRE ORGANISATION]` verlangt für den Zugriff auf alle dienstlichen Systeme und Anwendungen eine Mehr-Faktor-Authentisierung (MFA), soweit technisch umsetzbar.
>
> **Umsetzung:** Zentraler Mechanismus für MFA ist die Passwortverwaltung heylogin, die für jede verwaltete Zugangsdatei by design eine Zwei-Faktor-Authentisierung erzwingt. Die Architektur von heylogin bindet die Entschlüsselung von Zugangsdaten an einen Hardware-Sicherheitschip im Smartphone (TPM-Chip) oder im Sicherheitsschlüssel des Nutzers (Besitzfaktor), der über Biometrie oder PIN entsperrt werden muss (inhärenter bzw. Wissensfaktor). Dadurch ist jede über heylogin durchgeführte Anmeldung inhärent zwei-faktor-authentisiert, ohne dass MFA je Dienst konfiguriert werden muss.
>
> Für Systeme, die zusätzliche Authentisierungsfaktoren unabhängig von der Passwortverwaltung unterstützen (z. B. TOTP, FIDO2 WebAuthn), sind diese zu aktivieren, sofern die Datenklassifizierung des Systems dies erfordert. TOTP-Geheimnisse sind, soweit unterstützt, in heylogin zu speichern und dort zu automatisieren.
>
> **Abdeckung:** Alle Systeme und Anwendungen, deren Zugangsdaten in heylogin verwaltet werden, sind durch den integrierten Zwei-Faktor-Mechanismus von heylogin abgedeckt. Ein separates Verzeichnis MFA-fähiger Dienste ist für in heylogin verwaltete Zugangsdaten daher nicht erforderlich.

4 Verwendung von Kryptografie

4.1 Kontext

Organisationen, die sensible Authentisierungsdaten speichern oder verarbeiten, müssen ihren Umgang mit Kryptografie dokumentieren. Da heylogin den kryptografischen Schutz der Zugangsdaten im Auftrag der Nutzer übernimmt, sollte dies in Ihrer Kryptografie-Richtlinie abgebildet werden.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.8.24 (Verwendung von Kryptografie)

4.2 Was heylogin bereitstellt

- **Ende-zu-Ende-Verschlüsselung:** symmetrische Verschlüsselung und Integritätssicherung der Tresorinhalte mit XSalsa20 + Poly1305
- **Asymmetrische Verschlüsselung:** Schlüsselaustausch und Verwaltung der Tresorschlüssel mit Curve25519
- **Transportverschlüsselung:** Verschlüsselung der Daten während der Übertragung mit TLS 1.3 / 1.2 (HSTS erzwungen)
- **Backup-Verschlüsselung:** Verschlüsselung serverseitiger Backups mit ChaCha20 + Poly1305
- **Schlüsselschutz:** Schutz des kryptografischen Ausgangsmaterials im Hardware Secure Element (Secure Enclave / TPM)

Das kryptografische Ausgangsmaterial wird im Sicherheitschip des Nutzergeräts erzeugt und verlässt diesen nie unverschlüsselt. Damit besteht Schutz gegen Offline-Brute-Force-Angriffe, die bei Architekturen mit Master-Passwort möglich sind.

4.3 Vorlage: Ergänzung der Kryptografie-Richtlinie

> **Kryptografischer Schutz von Authentisierungsinformationen**
>
> Authentisierungsinformationen, die über die Passwortverwaltung der Organisation (heylogin) verwaltet werden, sind durch Ende-zu-Ende-Verschlüsselung geschützt. Die Verschlüsselung erfolgt clientseitig auf dem Gerät des Nutzers, bevor Daten an den Dienstleister übertragen werden. Es gelten die folgenden kryptografischen Maßnahmen:
>
> - **Vertraulichkeit:** Stromchiffre XSalsa20 mit Nachrichtenauthentisierung Poly1305 (AEAD-Konstruktion)
> - **Schlüsselaustausch:** Diffie-Hellman auf der elliptischen Kurve Curve25519
> - **Transport:** TLS 1.3 oder 1.2 mit erzwungenem HSTS
> - **Schutz des Schlüsselmaterials:** Erzeugung und Speicherung des kryptografischen Ausgangsmaterials im Hardware-Sicherheitschip des Geräts (Secure Enclave unter iOS, StrongBox/TEE unter Android oder FIDO2-Authenticator). Schlüsselmaterial liegt außerhalb des Sicherheitschips nie unverschlüsselt vor.
>
> Der Anbieter (heylogin GmbH) hat keine technische Möglichkeit, auf die Verschlüsselungsschlüssel oder die unverschlüsselten Inhaltsdaten zuzugreifen. Diese Zero-Knowledge-Architektur stellt sicher, dass eine Kompromittierung der Infrastruktur des Anbieters die

> Vertraulichkeit der gespeicherten Zugangsdaten nicht beeinträchtigt.
>
> Die eingesetzten kryptografischen Verfahren entsprechen dem aktuellen Stand der Technik. Die heylogin GmbH dokumentiert ihre kryptografische Architektur in einem öffentlich verfügbaren Security Whitepaper.

5 Personalmanagement: Onboarding und Offboarding

5.1 Kontext

Die Einführung einer Passwortverwaltung wirkt sich auf das Onboarding und Offboarding von Beschäftigten aus. Diese Prozesse müssen dokumentiert werden, um eine einheitliche Bereitstellung und *insbesondere* einen vollständigen Entzug der Zugriffe beim Austritt sicherzustellen.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.6.01 (Sicherheitsüberprüfung), A.6.02 (Beschäftigungs- und Vertragsbedingungen), A.6.05 (Verantwortlichkeiten bei Beendigung oder Änderung des Beschäftigungsverhältnisses), A.5.18 (Zugangsrechte)

5.2 Was heylogin bereitstellt

- **Onboarding:** Administratoren laden Nutzer per E-Mail in die Organisation ein. Nutzer richten heylogin ein, indem sie ihr Smartphone (oder einen FIDO2-Schlüssel) per QR-Code mit der Browsererweiterung koppeln. Teamzugehörigkeiten und Rollen werden von den Team-Administratoren zugewiesen.
- **Offboarding:** Administratoren können ein Nutzerkonto deaktivieren, wodurch weitere Synchronisation und Zugriffe unmittelbar unterbunden werden. Zugangsdaten in geteilten Teams bleiben für die übrigen Teammitglieder verfügbar. Hatte die austretende Person persönliche Zugangsdaten für Konten der Organisation, sollten diese gewechselt werden.
- **Kontowiederherstellung:** Administratoren der Organisation können eine Kontowiederherstellung für Nutzer anstoßen, die ihr Gerät verloren haben, ohne dabei Zugriff auf die Tresorinhalte zu erhalten.

5.3 Vorlage: Ergänzungen der Onboarding-Checkliste

Einrichtung der Passwortverwaltung (heylogin):

- ☐ Beschäftigte Person wurde in die heylogin-Organisation eingeladen
- ☐ Beschäftigte Person hat die heylogin-App auf dem Smartphone und die Browsererweiterung installiert
- ☐ Beschäftigte Person hat die Kopplung abgeschlossen (Scan des QR-Codes)
- ☐ Beschäftigte Person wurde den relevanten heylogin-Teams und Rollen zugewiesen
- ☐ Beschäftigte Person wurde über die Richtlinie zur Passwortverwaltung informiert
- ☐ Beschäftigte Person hat bestätigt, dass keine dienstlichen Zugangsdaten außerhalb von heylogin gespeichert werden
- ☐ Private Zugangsdaten werden über den privaten Account getrennt von der Organisation gespeichert

5.4 Vorlage: Ergänzungen der Offboarding-Checkliste

Entzug der Passwortverwaltung (heylogin):

- ☐ Das heylogin-Konto der beschäftigten Person wurde durch eine Administration der Organisation deaktiviert
- ☐ Die beschäftigte Person wurde aus allen heylogin-Teams entfernt
- ☐ Für Zugangsdaten geteilter Konten, auf die die beschäftigte Person Zugriff hatte, wurde die Notwendigkeit eines Wechsels bewertet
- ☐ Persönliche Zugangsdaten für Konten der Organisation wurden identifiziert und, soweit erforderlich, gewechselt
- ☐ Die beschäftigte Person wurde darüber informiert, dass der private Tresor (private, nicht organisationsbezogene Zugangsdaten) über den privaten heylogin-Account weiterhin zugänglich bleibt

5.5 Vorlage: Verfahren bei Geräteverlust

Verlust oder Diebstahl eines Geräts (Smartphone oder Sicherheitsschlüssel zur Nutzung von heylogin):

1. Die beschäftigte Person meldet den Verlust unverzüglich an `[IHRE IT-ANSPRECHSTELLE / ROLLE]`.
2. Eine heylogin-Administration entzieht dem verlorenen Gerät ohne Verzug den Zugriff.
3. War das verlorene Gerät der einzige Authenticator der beschäftigten Person, wird die

> Kontowiederherstellung durch eine Administration der Organisation angestoßen.
> 4. Die beschäftigte Person richtet heylogin auf einem Ersatzgerät ein.
> 5. Es ist zu bewerten, ob ein Wechsel der Zugangsdaten angezeigt ist, abhängig von den Umständen des Verlusts (z. B. Gerät war beim Diebstahl entsperrt).

6 Behandlung von Informationssicherheitsvorfällen

6.1 Kontext

Ihr ISMS muss festlegen, wie Sicherheitsvorfälle bei Lieferanten erkannt, kommuniziert und innerhalb der Organisation behandelt werden. Dieser Abschnitt beschreibt, wie heylogin Vorfälle kommuniziert und wie sich dies in Ihr eigenes Verfahren zur Vorfallbehandlung einbinden lässt.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.5.24 (Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen), A.5.25 (Beurteilung und Entscheidung über Informationssicherheitsereignisse), A.5.26 (Reaktion auf Informationssicherheitsvorfälle)

6.2 Was heylogin bereitstellt

- **Statusseite:** Der Dienststatus und Vorfälle werden öffentlich unter status.heylogin.com kommuniziert.
- **Klassifizierung von Vorfällen:** heylogin klassifiziert Vorfälle nach Schweregrad (0 = geringe oder keine Auswirkung, 1 = moderate Auswirkung auf die Verfügbarkeit oder geringe Auswirkung auf Vertraulichkeit/Integrität, 2 = erhebliche Auswirkung auf die Verfügbarkeit oder moderate Auswirkung auf Vertraulichkeit/Integrität).
- **Reaktion auf Vorfälle:** Das Betriebsteam von heylogin untersucht Vorfälle, ermittelt die Ursache, begrenzt die Auswirkungen und leitet Korrekturmaßnahmen ein. Vorfallberichte werden intern dokumentiert.
- **Meldung von Datenschutzverletzungen:** Bei einer Verletzung des Schutzes personenbezogener Daten informiert die heylogin GmbH betroffene Kunden innerhalb von 24 Stunden nach Kenntniserlangung, damit die 72-Stunden-Meldefrist nach Art. 33 DSGVO eingehalten werden kann.
- **Überwachung rund um die Uhr:** Die Produktivumgebung wird fortlaufend überwacht (minütlich). Für die Reaktion auf Vorfälle steht jederzeit eine Rufbereitschaft zur Verfügung.

- **Schwachstellenmeldung:** Externe Sicherheitsforschende können Schwachstellen unter einer öffentlichen Vulnerability Disclosure Policy (heylogin.com/de/schwachstellenmeldung) an security@heylogin.com melden.

6.3 Vorlage: Verfahren zur Behandlung von Vorfällen beim Lieferanten

> **Behandlung von Sicherheitsvorfällen beim Anbieter der Passwortverwaltung**
>
> **Überwachung:** `[VERANTWORTLICHE ROLLE]` prüft regelmäßig die Statusseite des heylogin-Dienstes unter status.heylogin.com. `[Zu prüfen: Abonnement der Benachrichtigungen der Statusseite, sofern verfügbar.]`
>
> **Beurteilung:** Kommuniziert heylogin einen Sicherheitsvorfall, bewertet `[VERANTWORTLICHE ROLLE]` dessen Relevanz und mögliche Auswirkungen auf `[IHRE ORGANISATION]`:
>
> - **Verfügbarkeitsvorfall:** Es ist festzustellen, ob der Geschäftsbetrieb betroffen ist. Zu beachten ist, dass die heylogin-Clients Zugangsdaten lokal zwischenspeichern, sodass kurze Störungen die Anmeldefähigkeit der Beschäftigten möglicherweise nicht beeinträchtigen.
> - **Vorfall betreffend Vertraulichkeit oder Integrität:** Es ist zu bewerten, ob die Zugangsdaten der Organisation betroffen sein können. Aufgrund der Zero-Knowledge- und Ende-zu-Ende-verschlüsselten Architektur führt eine serverseitige Kompromittierung bei heylogin nicht zur Offenlegung von Inhalten der Zugangsdaten. Betrifft der Vorfall clientseitige Schwachstellen oder eine Kompromittierung der Verschlüsselungsarchitektur, ist dies als Ereignis mit hohem Schweregrad zu behandeln und ein Wechsel der Zugangsdaten einzuleiten.
>
> **Eskalation:** Ergibt die Beurteilung eine wesentliche Auswirkung auf die Informationssicherheit der Organisation, ist ein Sicherheitsereignis gemäß dem Standardverfahren der Organisation zur Vorfallbehandlung (`[VERWEIS]`) zu erfassen.
>
> **Datenschutzverletzung:** Informiert die heylogin GmbH die Organisation über eine Verletzung des Schutzes personenbezogener Daten, bewertet `[VERANTWORTLICHE ROLLE]` unverzüglich, ob eine Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO erforderlich ist, und benachrichtigt betroffene Personen, sofern dies nach Art. 34 DSGVO erforderlich ist.

7 Business Continuity

7.1 Kontext

Die Verfügbarkeit Ihrer Passwortverwaltung beeinflusst unmittelbar die Fähigkeit der Beschäftigten, auf Geschäftssysteme zuzugreifen. Ihre Business-Impact-Analyse und Ihre Kontinuitätspläne sollten das Szenario einer Störung des heylogin-Dienstes berücksichtigen.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.5.29 (Informationssicherheit bei Störungen), A.5.30 (IKT-Bereitschaft für Business Continuity)

7.2 Was heylogin bereitstellt

- **Vertraglich zugesicherte Verfügbarkeit:** 99 % im Jahresmittel
- **Nachgewiesene Verfügbarkeit:** ca. 99,95 % im Jahresmittel
- **Recovery Time Objective (RTO):** 8 Stunden (definiert); < 2 Stunden (gemessen)
- **Recovery Point Objective (RPO):** 60 Minuten (stündliche verschlüsselte Backups)
- **Standby-Server:** geografisch getrenntes Rechenzentrum (Falkenstein); Umschaltung innerhalb von 30 Minuten
- **Clientseitiges Caching:** Zugangsdaten werden lokal in der Browsererweiterung und der mobilen App zwischengespeichert
- **Datenreplikation:** fortlaufende Replikation auf den Standby-Server über einen VPN-Tunnel

Das lokale Caching ist für die Business Continuity besonders relevant: Selbst bei einem vollständigen Ausfall der heylogin-Server können Beschäftigte weiterhin auf Zugangsdaten zugreifen, die zuvor mit ihren Geräten synchronisiert wurden.

7.3 Vorlage: Eintrag in der Business-Impact-Analyse

> - **System:** heylogin (Passwortverwaltung für Unternehmen)
> - **Unterstützte Geschäftsprozesse:** Authentisierung an allen Systemen und Anwendungen, deren Zugangsdaten in heylogin verwaltet werden
> - **Auswirkung einer Nichtverfügbarkeit:** `[Bewertung, z. B.: "Beschäftigte können nicht auf neue oder kürzlich geänderte Zugangsdaten zugreifen. Bereits synchronisierte Zugangsdaten bleiben lokal verfügbar. Die Auswirkung ist bei kurzen Störungen (< 4 Stunden) moderat und bei`

```
längeren Störungen hoch."]
```

- **RTO des Anbieters:** < 2 Stunden (gemessen), 8 Stunden (vertraglich)
- **RPO des Anbieters:** 60 Minuten
- **Kontinuitätsmaßnahmen:** Die mobilen Client-Apps von heylogin halten einen lokalen Cache der Zugangsdaten vor. Dies mindert die Auswirkung kurzer Dienststörungen.

8 Datenschutz und DSGVO

8.1 Kontext

Die DSGVO bildet die Grundlage aller Regelungen, insbesondere im Bereich der Passwortsicherheit. Da heylogin personenbezogene Daten im Auftrag Ihrer Organisation verarbeitet (mindestens E-Mail-Adressen der Beschäftigten und Metadaten zur Nutzung von Zugangsdaten), muss dies in Ihrer Datenschutzdokumentation abgebildet werden, einschließlich des Verzeichnisses von Verarbeitungstätigkeiten und der Auftragsverarbeitungsverträge.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.5.34 (Privatsphäre und Schutz von personenbezogenen Daten)

8.2 Was heylogin bereitstellt

- **Auftragsverarbeitungsvertrag (AVV)** verfügbar unter heylogin.com/de/avv; tritt automatisch mit Vertragsschluss in Kraft; beidseitige Signatur auf Anfrage möglich.
- **Ort der Verarbeitung:** ausschließlich Deutschland. Keine außereuropäischen Cloud-Anbieter für den Kerndienst.
- **Zero-Knowledge-Architektur:** Inhaltsdaten (Passwörter, Zugangsdaten) sind Ende-zu-Ende verschlüsselt und für die heylogin GmbH nicht zugänglich. Der Anbieter verarbeitet ausschließlich verschlüsselte Daten und begrenzte Metadaten (z. B. E-Mail-Adressen, Organisationszugehörigkeit).
- **Keine Tracker.** Die mobilen Apps von heylogin enthalten keine Werbe- oder Profiling-Tracker. Das Crash-Reporting ist pseudonymisiert, opt-in-basiert und zweckgebunden.
- **Rechte betroffener Personen:** Nutzer können ihre Daten exportieren. Löschanfragen werden auf Anfrage beim Support organisatorisch bearbeitet.
- **Keine Leistungsüberwachung.** Audit-Logs werden ausschließlich für Zwecke der IT-Sicherheit und Compliance verwendet. Eine Nutzung zur Leistungs- oder Verhaltenskontrolle ist vertraglich ausgeschlossen.

- **Schutz des privaten Tresors.** Administratoren haben keinen Zugriff auf und keine Einsicht in die privaten Tresordaten der Beschäftigten, einschließlich der Metadaten.
- **Betriebsratstauglichkeit.** Die externe Datenschutzprüfung durch die Projekt 29 GmbH & Co. KG bestätigt ausdrücklich die Vereinbarkeit mit den Anforderungen des Beschäftigtendatenschutzes und der Mitbestimmung.

8.3 Vorlage: Eintrag im Verzeichnis von Verarbeitungstätigkeiten

> - **Verarbeitungstätigkeit:** Passwortverwaltung für Unternehmen
> - **Zweck:** sichere Speicherung und Verwaltung von Authentisierungsinformationen für Systeme und Anwendungen der Organisation
> - **Rechtsgrundlage:** Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Informationssicherheit) oder Art. 6 Abs. 1 lit. b DSGVO (Erfüllung des Arbeitsvertrags)
> - **Kategorien betroffener Personen:** Beschäftigte, freie Mitarbeitende
> - **Kategorien personenbezogener Daten:** E-Mail-Adresse, Name, Organisationszugehörigkeit, verschlüsselte Zugangsdaten (für den Auftragsverarbeiter aufgrund der Ende-zu-Ende-Verschlüsselung nicht zugänglich)
> - **Empfänger:** heylogin GmbH (Auftragsverarbeiter); Unterauftragsverarbeiter gemäß Dokumentation unter heylogin.com/de/avv
> - **Drittlandübermittlungen:** keine für den Kerndienst. Optionale Nebenleistungen (z. B. Abrechnung) sind, soweit einschlägig, durch Angemessenheitsbeschlüsse oder Standardvertragsklauseln abgesichert
> - **Speicherdauer:** entsprechend der Vertragsdauer; Löschung bei Vertragsende und auf Anfrage
> - **Technische und organisatorische Maßnahmen:** Ende-zu-Ende-Verschlüsselung (Zero-Knowledge), ISO 27001-zertifizierter Anbieter, Datenverarbeitung in Deutschland, AVV geschlossen
> - **Verweis auf den AVV:** `[IHR Verweis, z. B. "geschlossen am DATUM, Version X"]`
> - **Verantwortlich:** `[NAME / ROLLE]`

9 Sensibilisierung und Schulung zur Informationssicherheit

9.1 Kontext

Organisationen müssen sicherstellen, dass Beschäftigte die Informationssicherheitsrichtlinien kennen und in den genutzten Werkzeugen geschult sind. Das Design von heylogin reduziert den Schulungsaufwand für Passwortsicherheit deutlich, was jedoch ausdrücklich dokumentiert werden sollte.

Relevante Maßnahmen nach ISO 27001:2022 Anhang A: A.6.03 (Informationssicherheitsbewusstsein, Ausbildung und Schulung)

9.2 Was heylogin bereitstellt

- **Keine Schulung zum Master-Passwort erforderlich.** Anders als herkömmliche Passwortmanager verwendet heylogin kein Master-Passwort. Beschäftigte müssen nicht darin geschult werden, ein Master-Passwort zu wählen, zu schützen oder zu wechseln.
- **Security by design.** Die Zwei-Faktor-Authentisierung ist Bestandteil der Architektur und keine optionale Konfiguration. Beschäftigte müssen MFA nicht separat aktivieren oder einrichten.
- **Phishing-Resistenz.** Das automatische Ausfüllen in heylogin ist domänengebunden und ersetzt den Anmeldevorgang im Browser. Dies verringert das Risiko der Eingabe von Zugangsdaten auf Phishing-Seiten.
- **Einfache Bedienung.** Das Interaktionsmodell “Swipe to Login” erfordert nur minimale Einarbeitung.

9.3 Vorlage: Ergänzung des Schulungsplans

> **Schulung zur Passwortverwaltung**
>
> Alle Beschäftigten erhalten im Rahmen des Onboardings eine Einführung in die Passwortverwaltung der Organisation (heylogin). Die Schulung umfasst:
>
> - Einrichtung und Kopplung von heylogin (Smartphone / Sicherheitsschlüssel und Browsererweiterung)
> - Speichern, Abrufen und Erzeugen von Zugangsdaten
> - Nutzung von heylogin-Teams für geteilte Zugangsdaten

- Die Pflicht, alle dienstlichen Zugangsdaten ausschließlich in heylogin zu speichern
- Vorgehen bei Verlust eines Geräts

Wiederkehrende Schulungen zu Themen der Passwortsicherheit (z. B. Umgang mit dem Master-Passwort, manuelle Einrichtung von MFA) sind **nicht erforderlich**, da heylogin starke, einmalige und hardwaregeschützte Zugangsdaten by design erzwingt. Sensibilisierungsmaßnahmen konzentrieren sich stattdessen auf das Erkennen von Social Engineering und die Meldung von Sicherheitsereignissen.

Verantwortlich: `[ROLLE]`

Häufigkeit: im Rahmen des Onboardings; Auffrischung als Teil `[IHRES jährlichen Sensibilisierungsprogramms]`

Anhang A: Zuordnung zu den Maßnahmen aus ISO 27001:2022 Anhang A

Die folgende Tabelle ordnet die Funktionen von heylogin einzelnen Maßnahmen aus ISO/IEC 27001:2022 Anhang A zu (abgeleitet aus ISO/IEC 27002:2022). Sie kann als Referenz beim Erstellen Ihrer Anwendbarkeitserklärung oder bei der Bewertung der Maßnahmenumsetzung dienen.

Maßnahme	Titel	Beitrag von heylogin
A.5.15	Zugangssteuerung	Zentrale Durchsetzung von Vorgaben für Zugangsdaten; teambasierter Zugriff mit administrativer Steuerung
A.5.16	Identitätsmanagement	Transparenz über geteilte Identitäten; Vergabe und Entzug von Zugriffen; Audit-Log

Maßnahme	Titel	Beitrag von heylogin
A.5.17	Authentisierungsinformationen	Automatische Erzeugung einmaliger starker Passwörter; verschlüsselte Speicherung und Übertragung; keine Verarbeitung im Klartext
A.5.19	Informationssicherheit in Lieferantenbeziehungen	heylogin ist nach ISO 27001:2022 zertifiziert; AVV verfügbar; Unterauftragsverarbeiter dokumentiert
A.5.23	Informationssicherheit bei der Nutzung von Cloud-Diensten	Zero-Knowledge-Architektur; Datenverarbeitung in Deutschland; clientseitige Verschlüsselung
A.5.24–28	Behandlung von Vorfällen	Öffentliche Statusseite; definierte Klassifizierung und Reaktion; Programm zur Schwachstellenmeldung
A.5.29–30	Business Continuity	Lokales Caching von Zugangsdaten; RTO < 2 h; RPO 60 min; geo-redundante Infrastruktur
A.5.34	Privatsphäre und Schutz von personenbezogenen Daten	AVV verfügbar; DSGVO-konform; Trennung des privaten Tresors; keine Leistungsüberwachung; externe Datenschutzprüfung

Maßnahme	Titel	Beitrag von heylogin
A.6.03	Bewusstsein, Ausbildung und Schulung	Reduziert den Schulungsaufwand (kein Master-Passwort, MFA by design); domänengebundenes Ausfüllen senkt das Phishing-Risiko
A.6.05	Verantwortlichkeiten bei Beendigung	Deaktivierung von Konten; Entfernen aus Teams; Vorgaben zum Wechsel von Zugangsdaten
A.8.02	Privilegierte Zugangsrechte	Privilegierte Zugangsdaten werden in heylogin mit demselben Schutzniveau verwaltet; administrative Übersicht ohne Inhaltszugriff
A.8.05	Sichere Authentisierung	Hardwaregestützte 2FA by design für alle Zugangsdaten; Biometrie/PIN bei jedem Zugriff erforderlich
A.8.24	Verwendung von Kryptografie	Ende-zu-Ende-Verschlüsselung (XSalsa20+Poly1305, Curve25519); Schlüsselspeicherung in Hardware; Transport über TLS 1.3/1.2

Anhang B: Zuordnung zu TISAX (VDA ISA)

Für Organisationen, die einer TISAX-Bewertung unterliegen, ordnet die folgende Tabelle die Funktionen von heylogin relevanten Kriterien des VDA ISA-Katalogs v5.0 zu.

VDA ISA	Kriterium	Beitrag von heylogin
3.1.4	Umgang mit mobilen IT-Geräten	heylogin nutzt Smartphones als Authenticator; eine Displaysperre mit Biometrie/PIN ist verpflichtend
4.1.2	Benutzerzugang zu Netzdiensten, IT-Systemen und IT-Anwendungen	2FA über das Smartphone ist für alle verwalteten Zugangsdaten in den Anmeldevorgang integriert
4.1.3	Sichere Verwaltung von Benutzerkonten und Anmeldeinformationen	Eindeutige persönliche Konten; die Ende-zu-Ende-Verschlüsselung verhindert Zugriffe des Anbieters; einfaches Offboarding; administrative Kontrolle über Sammelkonten
4.2.1	Vergabe und Verwaltung von Zugangsrechten	Passwörter sind aufgrund der Ende-zu-Ende-Verschlüsselung nur den Nutzern bekannt; teambasierte Freigabe mit administrativer Steuerung
5.1.1	Verwaltung kryptografischer Verfahren	XSalsa20+Poly1305 und Curve25519; dokumentiert im öffentlich verfügbaren Security Whitepaper
5.1.2	Schutz von Informationen beim Transport	Die Ende-zu-Ende-Verschlüsselung stellt sicher, dass nur Sender und Empfänger auf die Daten zugreifen können; TLS auf der Transportschicht

Anhang C: Wichtige Verweise und Kontaktpunkte

Ressource	Fundstelle
Security Whitepaper	heylogin.com/de/trust-center
Compliance Whitepaper	heylogin.com/de/trust-center
Auftragsverarbeitungsvertrag (AVV)	heylogin.com/de/avv
Datenschutzerklärung (Produkt)	heylogin.com/de/datenschutz
Liste der Unterauftragsverarbeiter	heylogin.com/de/avv
ISO 27001-Zertifikat	heylogin.com/de/trust-center
Dienststatus	status.heylogin.com
Schwachstellenmeldung	heylogin.com/de/schwachstellenmeldung
Sicherheitskontakt	security@heylogin.com
Rechtlicher Kontakt	legal@heylogin.com
Allgemeiner Support	support@heylogin.com