

Leistungsbeschreibung -- Managed Service Password Management

EXT IT GmbH -- Vahrenwalder Str. 271, 30179 Hannover

Hinweis: Diese Leistungsbeschreibung richtet sich ausschließlich an Unternehmer i.S.d. § 14 BGB. Verträge mit Verbrauchern i.S.d. § 13 BGB werden nicht geschlossen.

1. Servicebezeichnung

Managed Service Password Management

2. Servicebeschreibung

Der Service Managed Service Password Management umfasst die Bereitstellung, Lizenzierung und den Betrieb des Zero-Knowledge-Passwortmanagers **heylogin** (heylogin GmbH, Braunschweig) für die Beschäftigten des Auftraggebers. EXT IT stellt die heylogin-Enterprise-Lizenzen je Benutzer bereit, betreibt die Kundenorganisation als delegierter Administrator und ist zentraler Ansprechpartner (Single Point of Contact) für den Service.

heylogin verschlüsselt die gespeicherten Zugangsdaten Ende-zu-Ende auf den Endgeräten der Nutzer -- ohne Master-Passwort, gebunden an die Sicherheitschips der Geräte. Weder heylogin noch EXT IT haben Zugriff auf die in den persönlichen Tresoren gespeicherten Zugangsdaten im Klartext.

Die Ersteinrichtung, die Migration bestehender Zugangsdaten, Schulungen sowie die Support-Bearbeitung sind **nicht** Bestandteil der laufenden Servicepauschale, sondern werden nach Aufwand bzw. als Projekt gesondert beauftragt (siehe §4 und §6). Der Auftraggeber kann den administrativen Zugriff von EXT IT jederzeit entziehen und den Service eigenständig weiternutzen (siehe §11.2).

3. Leistungsumfang

3.1 Basisleistungen

- **Bereitstellung und Lizenzierung** von heylogin Enterprise je Benutzer.

- **Betrieb der Kundenorganisation** auf der heylogin-Plattform durch EXT IT als delegierter Administrator (technischer Plattformbetrieb im zur Service-Erbringung erforderlichen Umfang).
- **Single Point of Contact:** EXT IT ist zentraler Ansprechpartner des Auftraggebers für den Service und koordiniert Anfragen an den Hersteller heylogin. Die inhaltliche Bearbeitung von Support-Anfragen erfolgt nach Aufwand (siehe §4 und §8).
- **Information** des Auftraggebers über relevante Plattform- und Unterauftragsverarbeiter-Änderungen.

3.2 Enthaltene Tätigkeiten

Tätigkeit	Beschreibung	Intervall
Lizenzbereitstellung	Bereitstellung und Verwaltung der heylogin-Enterprise-Lizenzen je Benutzer	Laufend
Plattformbetrieb	Betrieb der Kundenorganisation als delegierter Administrator	Laufend
Single Point of Contact	Zentraler Ansprechpartner; Koordination von Anfragen an den Hersteller	Bei Bedarf

4. Leistungsabgrenzung

Folgende Leistungen sind **nicht** in der laufenden Servicepauschale enthalten und können gesondert beauftragt werden:

- **Ersteinrichtung/Onboarding** der Kundenorganisation und **Migration** bestehender Zugangsdaten (aus Altsystemen, anderen Passwortmanagern oder per CSV) -- als einmaliges Projekt nach Aufwand (Professional Services, abrufbar unter ext-it.tech/leistungen).
- **Support-Bearbeitung** (First-Level-Support-Anfragen, Konfigurationsänderungen, Störungsbearbeitung) -- nach Aufwand. Ein Freikontingent (z.B. ein Support-Ticket pro Monat) ist **nur enthalten, soweit es im individuellen Angebot bzw. Einzelauftrag ausdrücklich vereinbart wird.**
- **Schulungen** (Administratoren und Endanwender) -- gesondertes Angebot.
- **Vollständige Benutzerverwaltung** (Anlage und Zuweisung von Benutzern, Pflege von Teams und Berechtigungen durch EXT IT) -- als Add-on „Full Managed“ (individuelles Angebot, siehe §6).
- **Breach Detection (Pwnitoning)** für Organisationen mit weniger als 50 Lizenzen -- Add-on (siehe §6); ab 50 Lizenzen ist Pwnitoning in heylogin Enterprise enthalten.

- **On-Premise-Backup** der Organisations-Logins -- Add-on (siehe §6).
- **Bereitstellung und Support der Endgeräte** der Nutzer (Smartphones, Security-Keys, Browser).
- **Support der in heylogin gespeicherten Drittanwendungen** selbst.
- **Wiederherstellung von Benutzerkonten ohne gültigen Backup-Code** -- technisch durch die Zero-Knowledge-Architektur ausgeschlossen (siehe §11.1).

5. Voraussetzungen und Mitwirkungspflichten

5.1 Technische Voraussetzungen

- Je Benutzer ein geeignetes Anmeldegerät: ein Smartphone (iOS ab Version 13 oder aktuelles Android) zur Swipe-to-Login-Bestätigung **oder** alternativ ein FIDO2-Security-Key; ergänzend nutzbar sind Touch ID (macOS) und Windows Hello.
- Ein aktueller Browser für die heylogin-Browser-Erweiterung (Chrome, Firefox, Safari, Edge) bzw. die heylogin-App (iOS/Android).
- Erreichbarkeit der heylogin-Dienste über HTTPS (Port 443; u.a. [heylogin.app](#), [*.heylogin.com](#)). In restriktiven Netzen ist die vom Hersteller bereitzustellende Freigabeliste (Allowlist) durch den Auftraggeber zu hinterlegen.
- Für die Verzeichnis-Synchronisation: Microsoft Entra ID (Admin-Consent mit den Berechtigungen `User.Read.All` und `Group.Read.All`) oder Google Workspace; alternativ CSV-Import.

5.2 Mitwirkungspflichten des Auftraggebers

- Benennung eines fachlichen Ansprechpartners mit Entscheidungsbefugnis.
- Bereitstellung der für die Verzeichnis-Synchronisation erforderlichen Admin-Freigaben (Entra-ID-Consent durch ein privilegiertes Konto) bzw. Pflege der CSV-Daten.
- Bereitstellung geeigneter Anmeldegeräte für die Nutzer sowie **sichere Verwahrung der Backup-/Wiederherstellungscodes** durch die Nutzer.
- Information über neue und ausscheidende Mitarbeiter (On-/Offboarding) zur Lizenz- und Benutzerpflege.
- Vorhalten **mindestens eines internen Administrators** beim Auftraggeber, um die jederzeitige Entkopplung des EXT-IT-Zugriffs zu ermöglichen (siehe §11.2).
- Freischaltung der heylogin-Dienste in restriktiven Netzen.

- Unverzögliche Meldung von Störungen über das Ticketsystem sowie Bereitstellung einer zentralen E-Mail-Adresse für Ankündigungen.

6. Optionale Zusatzleistungen

Zusatzleistung	Beschreibung	Abrechnungsmodell
Full Managed	Vollständige Benutzer- und Tenant-Verwaltung: Anlage und Zuweisung von Benutzern, Pflege von Teams und Berechtigungen durch EXT IT	Individuelles Angebot
Breach Detection (Pwnitring)	Domainbasiertes Leak-Monitoring für Organisationen mit weniger als 50 Lizenzen (ab 50 Lizenzen in Enterprise enthalten)	Jährliche Pauschale je Organisation
On-Premise-Backup	Verschlüsseltes Backup der Organisations-Logins auf einem Server des Auftraggebers (mind. 50 Lizenzen)	Monatliche Pauschale je Benutzer
Zusätzlicher delegierter Administrator	Weiterer administrativer EXT-IT-Zugang über den standardmäßig einen Administrator hinaus	Pauschale
Ersteinrichtung & Migration	Einrichtung der Organisation, Verzeichnis-Anbindung, Rollout, Import bestehender Zugangsdaten	Projekt nach Aufwand
Schulung	Administrator- und Endanwender-Schulung	Nach Aufwand / Angebot
Support	First-Level-Support, Konfigurationsänderungen, Störungsbearbeitung	Nach Aufwand (Freikontingent nur, soweit im Angebot vereinbart)

7. Service Level

Es gelten die Servicezeiten und allgemeinen Regelungen gemäß §6a der Allgemeinen Geschäftsbedingungen (abrufbar unter [ext-it.tech/agb/](https://www.ext-it.tech/agb/)).

Produktspezifische Verfügbarkeit: Die Verfügbarkeit der Passwortmanager-Plattform richtet sich nach dem Betrieb des Herstellers heylogin (Wiederherstellungsziele laut Hersteller: RTO 8 Stunden, RPO 60 Minuten); eine eigenständige Verfügbarkeitszusage durch EXT IT besteht nicht. Ausfälle der heylogin-Plattform liegen gemäß §6a Abs. 3 lit. d AGB außerhalb des Einflussbereichs von EXT IT.

Die Bearbeitung von Support-Anfragen erfolgt nach Aufwand im Rahmen der Servicezeiten gemäß §6a AGB; ein darüber hinausgehendes, produktspezifisches Reaktionszeit-SLA besteht nicht. Service Credits oder Vertragsstrafen sind nicht vereinbart.

8. Vergütung

Modell	Beschreibung
Pauschale je Benutzer	Enthält die heylogin-Enterprise-Lizenz und den Plattformbetrieb durch EXT IT als delegierter Administrator. Die Abrechnung erfolgt jährlich im Voraus ; unterjährig hinzukommende Benutzer werden anteilig berechnet.
Ersteinrichtung & Migration	Einmaliges Projekt nach Aufwand bzw. Pauschalangebot (siehe §4).
Support	Nach Aufwand zum im Angebot vereinbarten Stundensatz gemäß §5 Abs. 3 AGB. Ein Freikontingent (z.B. ein Ticket pro Monat) ist nur enthalten, soweit im individuellen Angebot bzw. Einzelauftrag ausdrücklich vereinbart.
Add-ons	Breach Detection, On-Premise-Backup, zusätzlicher delegierter Administrator und Full Managed gemäß individuellem Angebot.
Mindestabnahme / Mindestlaufzeit	Keine Mindestabnahme an Benutzern. Mindestlaufzeit 12 Monate (siehe §12).

Aktuelle Preise erhalten Sie auf Anfrage oder in Ihrem individuellen Angebot.

9. Vertragliche Grundlagen

Dokument	Abruf
Allgemeine Geschäftsbedingungen	ext-it.tech/agb/
Auftragsverarbeitungsvertrag	ext-it.tech/avv
Produktspezifische AVV-Anlage 2 -- Managed Service Password Management	ext-it.tech/avv

10. Datenschutz (AVV)

Im Rahmen des Managed Service Password Management werden personenbezogene Daten des Auftraggebers verarbeitet (insbesondere Benutzerkennungen und E-Mail-Adressen, Team- und Berechtigungsstrukturen, Geräte- und Browserinformationen

sowie Zugriffs- und Audit-Logs einschließlich IP-Adressen). Die Verarbeitung erfolgt auf Grundlage des Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DSGVO.

Die in den Tresoren gespeicherten Zugangsdaten selbst (Benutzernamen, Passwörter, Schlüssel) werden Ende-zu-Ende auf den Endgeräten der Nutzer verschlüsselt und sind weder für heylogin noch für EXT IT im Klartext zugänglich. Die Verarbeitung der Plattformdaten erfolgt ausschließlich in Deutschland.

Alle relevanten Datenschutz-Dokumente sind unter ext-it.tech/avv abrufbar:

- AVV-Rahmenvertrag
- Produktspezifische Anlage 2 -- Managed Service Password Management
- Technisch-organisatorische Maßnahmen (Anlage 1)
- Zentrale Unterauftragsverarbeiter-Liste (Anlage 3)

Der AVV wird automatisch Vertragsbestandteil bei Beauftragung (siehe §1 Abs. 2 AVV).

11. Besonderheiten dieses Services

11.1 Zero-Knowledge-Architektur und Wiederherstellungscodes

heylogin verschlüsselt die Zugangsdaten Ende-zu-Ende ohne Master-Passwort; der Zugang ist an die Sicherheitschips (Secure Enclave/TPM) der Anmeldegeräte gebunden. Gehen alle Anmeldegeräte eines Nutzers verloren und liegt **kein gültiger Backup-/Wiederherstellungscodes** vor, ist eine Wiederherstellung der betroffenen Zugangsdaten **technisch ausgeschlossen** -- weder durch EXT IT noch durch heylogin.

Der Auftraggeber stellt sicher, dass seine Nutzer Backup-/Wiederherstellungscodes sicher verwahren und dass mindestens ein interner Administrator vorhanden ist. Eine Haftung von EXT IT für einen derart bedingten Datenverlust ist im Rahmen des §7 AGB ausgeschlossen.

11.2 Jederzeitige Entkopplung des EXT-IT-Zugriffs

Der Auftraggeber kann den administrativen Zugriff von EXT IT jederzeit entziehen, indem die delegierten Administratoren entfernt und die Organisation auf der heylogin-Plattform in eine unabhängige Organisation umgewandelt wird (Voraussetzung: mindestens ein interner Administrator des Auftraggebers). Der Service kann anschließend regulär weitergenutzt werden; die vereinbarte Vergütung und Mindestlaufzeit bleiben hiervon unberührt.

11.3 Keine SSO-/SCIM-Föderation

heylogin unterstützt kein SAML/SSO und kein SCIM. Die Benutzer-Synchronisation erfolgt über Microsoft Entra ID, Google Workspace oder CSV-Import. Bei Einsatz eines anderen Identity-Providers ist eine manuelle bzw. CSV-basierte Benutzerpflege erforderlich.

12. Laufzeit und Kündigung

Es gelten die Regelungen des §10 der Allgemeinen Geschäftsbedingungen (abrufbar unter ext-it.tech/agb/). Die Mindestlaufzeit beträgt 12 Monate bei jährlicher Vorauszahlung; abweichende Laufzeiten und Kündigungsfristen können im jeweiligen Einzelauftrag individuell vereinbart werden. Die Regelung zur Entkopplung des EXT-IT-Zugriffs (§11.2) bleibt von der Kündigung unberührt.

Änderungshistorie

Version	Datum	Änderung	Verantwortlich
1.0	2026-06-01	Erstveröffentlichung	Geschäftsführung

Stand: 2026-06-01