**Lastenheft für**

**IAM System in der AMEOS Gruppe**

Inhaltsverzeichnis

[1 Einleitung 4](#_Toc173505161)

[1.1 Präsentation des Unternehmens 4](#_Toc173505162)

[1.2 Übersicht der Stakeholder 5](#_Toc173505163)

[1.3 AMEOS Struktur 5](#_Toc173505164)

[2 Rahmenbedingungen 6](#_Toc173505165)

[2.1 Ausgangssituation 6](#_Toc173505166)

[2.2 Strategische Ziele 6](#_Toc173505167)

[2.3 Operative Ziele 7](#_Toc173505168)

[2.4 Vision 7](#_Toc173505169)

[2.5 Ist-Zustand 8](#_Toc173505170)

[3 Produkteinsatz / Anwendungsbereiche 8](#_Toc173505171)

[3.1 Anwendungsbereich 8](#_Toc173505172)

[3.2 Zielbenutzergruppen 9](#_Toc173505173)

[3.3 Verfügbarkeit des Produktes (SLA) 9](#_Toc173505174)

[4 Kriterienkatalog 9](#_Toc173505175)

[4.1 Allgemein 10](#_Toc173505176)

[4.2 Support 10](#_Toc173505177)

[4.3 Schulung 11](#_Toc173505178)

[4.4 Ergänzungen 12](#_Toc173505179)

[4.5 Datensicherheit / Rechtekonzept 12](#_Toc173505180)

[4.6 Leistungsanforderungen 13](#_Toc173505181)

[4.7 Systemarchitektur 13](#_Toc173505182)

[4.8 Verfügbarkeit des Systems 14](#_Toc173505183)

[4.9 Schnittstellen / Kompatibilität 14](#_Toc173505184)

[4.10 Systemanforderungen 15](#_Toc173505185)

[4.11 Softwarepflege 15](#_Toc173505186)

[4.12 Anwendungsfall 16](#_Toc173505187)

[5 Produktanforderungen 16](#_Toc173505188)

[5.1 Funktionale Anforderungen 16](#_Toc173505189)

[Eintritt 17](#_Toc173505190)

[Berechtigungsrelevante Veränderung 17](#_Toc173505191)

[Nicht-Berechtigungsrelevante Veränderung 17](#_Toc173505192)

[Austritt 17](#_Toc173505193)

[Pausen und ruhende Arbeitsverhältnisse 17](#_Toc173505194)

[Nutzer ohne Active Directory Account 18](#_Toc173505195)

[Digitaler „Laufzettel“ 18](#_Toc173505196)

[Synchronisationszeitpunkt 18](#_Toc173505197)

[5.2 Nichtfunktionale Anforderungen 18](#_Toc173505198)

[5.3 Technische Anforderungen 19](#_Toc173505199)

[5.3.1 Allgemeine Anforderungen 19](#_Toc173505200)

[5.3.2 Schnittstellen und Kompatibilität 19](#_Toc173505201)

[5.3.3 Systemanforderungen - IT 20](#_Toc173505202)

[5.3.4 Unterlagen die mit Inbetriebnahme zur Verfügung zu stellen sind 21](#_Toc173505203)

[6 Soll – Zustand 21](#_Toc173505204)

[7 Zukünftige Erweiterungen 21](#_Toc173505205)

[8 Schulungen / Dokumentation 21](#_Toc173505206)

[9 Service / Support / Updates 22](#_Toc173505207)

[10 Voraussichtliches Mengengerüst 22](#_Toc173505208)

[11 Projektablauf 23](#_Toc173505209)

[11.1 Zeitrahmen 23](#_Toc173505210)

[11.2 Geplanter Ablauf 23](#_Toc173505211)

[11.3 IAM Schnittstellen und Funktionalitäten Mindestumfang: 24](#_Toc173505212)

[11.4 Rolloutplan des KHZG-Programms 25](#_Toc173505213)

[12 Hinweis 25](#_Toc173505214)

# Einleitung

## Präsentation des Unternehmens

AMEOS sichert die Gesundheitsversorgung in den Regionen.

Die AMEOS Gruppe zählt zu den wichtigen Gesundheitsversorgern im deutschsprachigen Raum. Wir stehen für Qualität, Innovation und Stabilität. Die 18.000 Mitarbeitenden verbindet ihre gemeinsame Mission: „Wir arbeiten für Ihre Gesundheit“.

Zur AMEOS Gruppe gehören 107 Einrichtungen an 60 Standorten, die insgesamt 10.000 Behandlungsplätze bieten. Die Mitarbeitenden unserer Krankenhäuser, Poliklinika, Reha-, Pflege- und Eingliederungseinrichtungen sichern die umfassende Gesundheitsversorgung für die Bevölkerung in den Regionen.

Die stetige Weiterentwicklung unserer Qualitätsstandards steht im Einklang mit den hohen Ansprüchen, die wir uns zum Ziel gesetzt haben. Wir verstehen Qualität als einen aktiven und kontinuierlichen Prozess. Damit gelingt es uns, ein Höchstmaß an Patientensicherheit, medizinischer Qualität und bestmöglicher Versorgung zu erreichen. Gut ausgebildete und motivierte Mitarbeitende sind dafür Voraussetzung. AMEOS sichert ihren Fachkräftebedarf über die vielfältigen Aus- und Weiterbildungsangebote ihrer Institute sowie über ein Netz von Lehrkrankenhäusern für Medizin und Pflege. Die individuelle Weiterentwicklung und Neugewinnung von qualifizierten Mitarbeitenden, die uns auf unserem Weg unterstützen, ist uns besonders wichtig.

Wir setzen Maßstäbe in der Gestaltung von Klinikums- und Zentrumsstrukturen. Dabei gehen wir außergewöhnliche Wege und definieren Abläufe sowie Zusammenhänge neu. Unser Ziel ist eine stabile und bedarfsgerechte regionale Versorgung anzubieten und damit unseren öffentlichen Versorgungsauftrag zu erfüllen. AMEOS investiert in die Entwicklung neuer und notwendiger Leistungsangebote an ihren Standorten. Die enge Zusammenarbeit mit den regionalen Entscheidungsträgern und unseren Partnern in der Wirtschaft ist ein wesentlicher Erfolgsfaktor.

Die besondere Stärke der AMEOS Gruppe wird durch die zentralen und regionalen Kompetenzzentren deutlich. Hier gelingt es die Einrichtungen von administrativen Prozessen zu entlasten und optimierte Standards und Best-Practice-Ansätze auf die gesamte Gruppe zu übertragen. Durch eine Unternehmenskultur, die Verantwortung und Engagement fördert, gestalten wir gemeinsam die Zukunft der AMEOS Gruppe. Alle Mitarbeitenden vereint dabei der Gedanke: Vor allem Gesundheit!

Die AMEOS Einrichtungen sind aufgeteilt in vier Regionen. In den jeweiligen Regionalzentralen bündeln wir unsere Kompetenzen in den Bereichen Einkauf, Finanzen, Kommunikation, Medizinentwicklung und Personal. Hier erfahren Sie mehr über die Regionen:

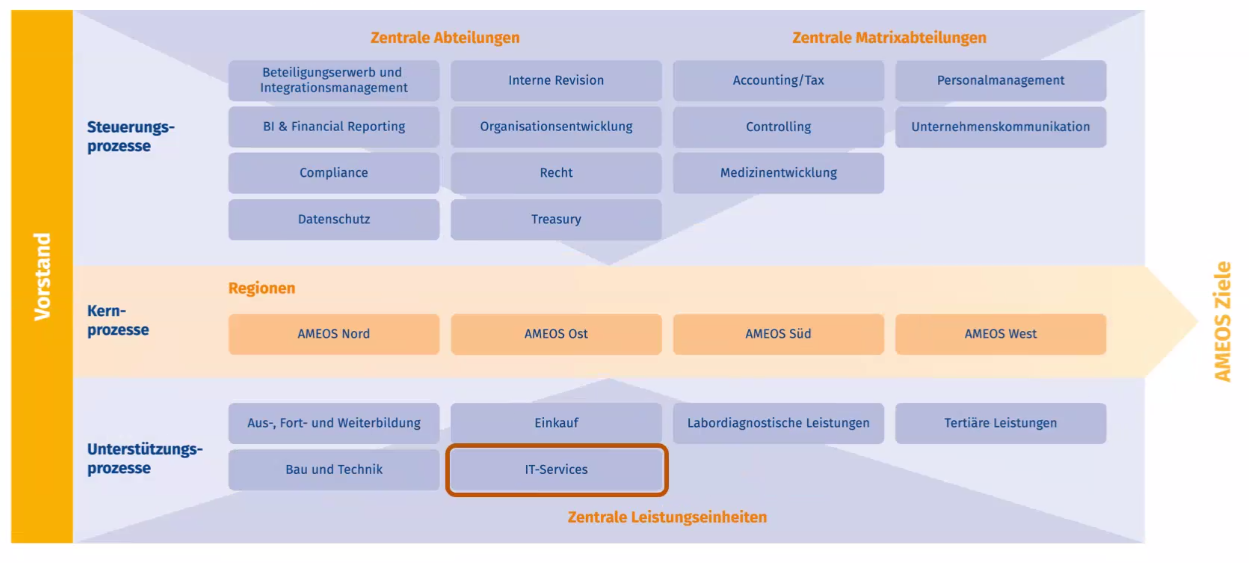
<https://www.ameos.eu/standorte/ueberblick/unsere-regionen/>

## Übersicht der Stakeholder

Verschiedene Stakeholder innerhalb der AMEOS Gruppe haben unterschiedliche Anforderungen an die erfolgreiche Einführung und Nutzung des IAM Systems. Stakeholder sind unter anderem

* *Krankenhausdirektoren*
* *Pflegedirektoren*
* *HR-Abteilung*
* *Organisationsentwicklung*
* *Medizinentwicklung*
* *IT-Abteilung*
* *Betriebsrat*
* *Vorstand*

## AMEOS Struktur



Zentrale Klammer über alle Einrichtungen und Bereiche ist die AMEOS Gruppe. Die Zentrale der Gruppe hat ihren Sitz in Zürich, wo der Vorstand sowie bestimmte Mitarbeitende angesiedelt sind. Die Einrichtungen sind in vier Regionen Nord, Ost, Süd und West geordnet.

Der Standort ist die Basis für die jeweiligen Einrichtungen der AMEOS Gruppe. Je Standort kann es mehrere unterschiedliche Einrichtungen geben. Je Einrichtungen gibt es unterschiedliche Anforderungen an die zu findenden Informationen.

Es gibt folgende Einrichtungsarten: Somatik, Psychiatrie Forensik, Eingliederung, ambulante und stationäre Pflege, Rehabilitation, Polikliniken (Medizinische Versorgungszentren MVZ), ambulante Therapien.

Neben den Einrichtungen gibt es Zentrale Leistungseinheiten, deren Mitarbeitende direkt am Standort als Dienstleister tätig sind, jedoch nicht direkt zu einer Einrichtung dazugehören. Diese müssen mit den örtlichen Standortinformationen versorgt werden und gleichzeitig muss eine eigene Informations-Plattform zur Verfügung gestellt werden. Dies sind bspw. IT-Services, Bau und Technik (Technikteams), Tertiäre Leistungen (Reinigungsdienstleistungen, Schreibdienst, Speiseversorgung etc.) und Labor

In den Matrixbereichen sind Kompetenzen/Themen gebündelt, die ein Pendent in der jeweiligen Regionalzentrale haben (z.B. Unternehmenskommunikation, Personalmanagement, Einkauf, Medizinentwicklung etc.). Diese arbeiten gemeinsam an Gruppenthemen zur Steuerung der Regionen und Einrichtungen.

# Rahmenbedingungen

## 2.1 Ausgangssituation

Die AMEOS Gruppe verfügt aktuell über keine zentrale Identitäts- und Zugriffsverwaltung (IAM). Einstellungen, Veränderungen oder Austritte von Mitarbeitenden verlangen eine Reihe von Maßnahmen, die oft individuell gesteuert sind und sich von Einrichtung zu Einrichtung unterscheiden.

Das Mitarbeitermanagement wird von unterschiedlichen Stellen aus gesteuert.

Einstellungen und Austritte initiiert die HR-Abteilung in der HR-Software LoGA der Fa. P&I. Entgeltrelevante Veränderungen von Mitarbeitern werden von der HR Abteilung in der HR Software initiiert. Veränderungen die nicht entgeltrelevant sind, werden durch die verantwortlichen Vorgesetzten in Dienstplansoftwaren initiiert. Einige Veränderungen resultieren in Tickets an die IT oder in Email Kommunikationen mit den Besitzern der bestimmten Teilprozesse. Daraus wiederum resultieren die notwendigen Schritte für die IT-Abteilung bei der Berechtigung der jeweiligen Mitarbeiter auf IT-Systeme.

In Summe ist der Mitarbeiterlebenszyklus gegenwärtig uneinheitlich und durch die diversen manuell durchgeführten Abläufe oft fehleranfällig oder unvollständig.

## 2.2 Strategische Ziele

Im Rahmen des KHZG plant AMEOS die Digitalisierung und Standardisierung der Geschäftsprozesse.

Neu gedachte und definierte Prozesse sollen implementiert und gelebt werden, um eine Vereinheitlichung herbeizuführen. Dies stellt die Grundlage dar, um auf zukünftige Herausforderungen im Krankenhausumfeld vorbereitet zu sein.

Die digitale Transformation der AMEOS Gruppe soll sukzessive bis 31.12.2025 abgeschlossen sein. In der Roadmap, siehe 11.4 Rolloutplan des KHZG-Programms, sind die einzelnen Standorte aufgeführt. Der geplante Projektablauf ist unter 11.2 abgebildet. Nicht aufgeführte Standorte können ab 2026 umgesetzt werden.

Ein IAM System ist eine zentrale Komponente der AMEOS IT-Sicherheitsstrategie zum Schutz von IT-Systemen und seine zentrale Aufgabe (Kernkompetenz) die Autorisierung von Benutzern. Einem Individuum wird eine digitale Identität zugewiesen, die über den gesamten Zugriffslebenszyklus eines Benutzers hinweg gewartet, aktualisiert und überwacht wird.

## 2.3 Operative Ziele

Ziel der Einführung eines IAM Systems ist die Harmonisierung, Automatisierung und Dokumentation von Geschäftsprozessen.

Im Rahmen eines vorgelagerten Projekts wird vom Auftraggeber über die verschiedenen Standorte und Mitarbeiterrollen eine Bestandsaufnahme und Dokumentation der Mitarbeiterprozesse durchgeführt. Eine Vereinheitlichung wird angestrebt.

Die vorab definierten Mitarbeiterrollen und Prozesse bilden die Basis des IAM Systems bzw. dessen Logik.

Das zentrale IAM System soll die verschiedenen Abteilungen bei Eintritt, Austritt und Veränderung von Mitarbeitern unterstützen. Ziel ist ein hoher Automatisierungsgrad um den Verwaltungsaufwand zu verringern und weitestgehend zu vereinheitlichen Dafür soll das System neben der Berechtigungssteuerung auch ausgewählte Businessprozesse unterstützen.

Das IAM soll zentral über alle aktuellen und zukünftigen AMEOS Standorte betrieben werden.

## 2.4 Vision

Für alle Bereiche und Standorte innerhalb der AMEOS Gruppe sind die notwendigen Prozessschritte definiert und im IAM funktional abgebildet. Dies umfasst den gesamten Lebenszyklus eines Mitarbeiters des Unternehmens, sowie zusätzlich die Verwaltung von externen Mitarbeitern, sowie Service-, Funktions- und privilegierten Accounts.

Das IAM System wird vom LoGA HR über Änderungen per API informiert und steuert automatisiert Maßnahmen ein. Grundlage sind vorab definierte Prozesse und Mitarbeiterrollen, die im IAM funktional abgebildet sind. Einstellungen, Entlassungen oder Veränderung von Personal werden durch das HR-Team oder die verantwortlichen Leiter im Krankenhaus im HR oder Dienstplan System gepflegt. Darauffolgende Aktivitäten im Mitarbeiterlebenszyklus werden vom IAM anhand der definierten Wege automatisch, bzw. unter Berücksichtigung von Prozessschritten, die eine Genehmigung erfordern, veranlasst, umgesetzt und revisionssicher dokumentiert.

Anhand regelmäßig automatisiert erstellter Reports ist es nachvollziehbar, welche Gruppen und Rollen zu welchem Zeitpunkt an welchen Mitarbeiter vergeben wurde. Dazu ist es möglich den aktuellen Stand der vergebenen Berechtigungen mit Freigebenden und Begründung zu ermitteln.

Weiterhin ist es für Mitarbeiter möglich, über das IAM mit Hilfe eines SelfService-Portals Passwortrücksetzung des eigenen User-Accounts durchzuführen.

Auch die erweiterte Anfrage von Mitarbeiterrollen, welche nicht in der Arbeitsplatzdefinition enthalten sind, kann von einem selbst, von anderen Mitarbeitenden oder von Vorgesetzten angefordert werden. Der Genehmigungsprozess wird für jede Mitarbeiterrolle ein- oder mehrstufig gestaltet werden.

Der Antragsteller und die Zielperson können den Fortschritt der Anfrage in Reporten einsehen und im System ggf. stornieren. Bei Genehmigung, Ablehnung und Stornierung werden die Mitarbeitenden und der Auftraggeber per E-Mail informiert. Vollständige Kontaktdaten werden durch entsprechende Pflichtfelder gewährleistet.

Rollen können von anderen Mitarbeitenden ausgewählt und kopiert werden. (Einkaufswagen-Prinzip: Mitarbeiter B kann sich die Berechtigungen von Mitarbeiter A anschauen und diese gezielt auswählen, beantragen und den Genehmigungsprozess starten)

Rollen haben rollenverantwortliche Besitzer, welche die vorhandenen Rollen regelmäßig im Rahmen eines Reviews auf Veränderungen in der Organisation oder der IT-Systeme überprüfen und notwendige Anpassungen umsetzen.

Support für hybride IT-Umgebungen, die On-Premise-Systeme und SaaS-Applikationen umfassen, soll langfristig möglich sein.

Audit-Funktionen leiten für Genehmigende, Fachbereichs- und Rollenverantwortliche in konfigurierbaren Abständen Überprüfungen von Gruppenzugehörigkeiten ein, sodass überflüssige Berechtigungen und Bereichswechsel entsprechend behandelt werden.

## 2.5 Ist-Zustand

Aktuell wird das Mitarbeitermanagement von unterschiedlichen Stellen gesteuert und ist über die verschiedenen Häuser unterschiedlich und uneinheitlich.

Einstellungen und Austritte initiiert die HR-Abteilung. Veränderungen, die nicht entgeltrelevant sind, werden durch die verantwortlichen Vorgesetzten in Dienstplansoftwaren initiiert. Entgeltrelevante Veränderungen von Mitarbeitern werden von HR initiiert. Veränderungen von Mitarbeitern resultieren in Tickets an die IT oder in Email Kommunikationen mit den Besitzern der bestimmten Teilprozesse.

Das zentrale HR-System der AMEOS ist die Software LoGA HR, die als SaaS Lösung zentral betrieben wird. Mit Hinterlegung des Eintrittsdatum werden zukünftig die Mitarbeiterdaten an das IAM übertragen werden. Entgeltrelevante Veränderungen werden durch die HR-Abteilung im LoGA HR eingepflegt. Neben der Steuerung aus dem HR-System müssen auch manuelle angesteuerte Schritte für die Berechtigungsvergabe möglich sein.

Austritte von Mitarbeitern werden durch die HR-Abteilung im LoGA HR eingepflegt. Zum Tag des Austritts werden dann manuelle Maßnahmen (Ticket an IT) eingesteuert, dass die Zugriffe entsprechend gesperrt oder entfernt werden. Bei Sofortaustritten wird direkt eine Sperrung der Zugriffe via Ticket veranlasst.

# Produkteinsatz / Anwendungsbereiche

## 3.1 Anwendungsbereich

Das IAM soll im Bereich der IT-Berechtigungsverwaltung und des Asset Managements (Handy-, PC-, Laptopbeschaffung) unterstützen. Es wird aufgrund seiner Funktion in zahlreiche Prozesse der AMEOS Gruppe eingreifen können. Mit zunehmender Digitalisierung und dem Einsatz zusätzlicher IT-Systeme wird der Anwendungsbereich der IAM Lösung entsprechend größer.

Im Rahmen der Ertüchtigung der AMEOS Standorte im KHZG Umfeld erweitert sich der Anwendungsbereich sukzessive. Das IAM System soll zentrale und dezentrale IT-Dienste an den Standorten ansteuern.

## 3.2 Zielbenutzergruppen

Das IAM soll in der gesamten AMEOS Gruppe Verwendung finden.

* + Regionen
  + Zentrale Leistungseinheiten
  + Zentrale Matrixabteilungen
  + Zentrale Abteilungen
  + Externe Dienstleister, die AMEOS Accounts nutzen

## 3.3 Verfügbarkeit des Produktes (SLA)

Eine 99,7%ige Verfügbarkeit ist gefordert. Diese bezieht sich auf das Softwareprodukt, vorausgesetzt, dass Ausfälle nicht durch die unterlagerte Infrastruktur ausgelöst wurden.

# Kriterienkatalog

Im Folgenden sind die Kriterien aufgeführt, welche die AMEOS Gruppe an ein IAM-System für die zur Verfügungsstellung einer zentrale Identitäts- und Zugriffsverwaltung fordert. Bitte geben Sie in Anlage 4 an, ob zum Zeitpunkt der Angebotsabgabe die Kriterien erfüllt sind inklusive eventueller Zusatzinformationen. Es wird zwischen folgenden Kriterien unterschieden:

* Ausschlusskriterien (A)
* Bewertungskriterien mit hoher Priorität (H)
* Bewertungskriterien mit niedriger Priorität (N)
* Informationskriterien (I) (ergänzende Informationen ohne Einfluss auf die Bewertung)

Im Rahmen der Angebotswertung werden für jedes erfüllte Bewertungskriterium mit hoher Priorität (H) 30 Punkte und mit niedriger Priorität (N) 6 Punkte vergeben. Bitte prüfen Sie Ihre Angaben und Antworten zu den Anforderungen der Ausschlusskriterien sorgfältig.

Die Kriterien/ Funktionsanforderungen unterteilen sich in folgende Gruppen

1. [Allgemein](#_Allgemein)
2. [Support](#_Support)
3. [Schulung](#_Schulung)
4. [Ergänzungen](#_Ergänzungen)
5. [Datensicherheit/Rechtekonzept](#_Datensicherheit_/_Rechtekonzept)
6. [Leistungsanforderungen](#_Leistungsanforderungen)
7. [Systemarchitektur](#_Systemarchitektur)
8. [Verfügbarkeit des Systems](#_Verfügbarkeit_des_Systems)
9. [Schnittstellen / Kompatibilität](#_Schnittstellen_/_Kompatibilität)
10. [Systemanforderungen](#_Systemanforderungen)
11. [Softwarepflege](#_Softwarepflege)
12. [Anwendungsfall](#_Anwendungsfall)

Anmerkung zu den folgenden Tabellen:

* In der Spalte „Kriterium Nr.“ ist die laufende Nummer der jeweiligen Anforderung angegeben.
* In der Spalte „Anforderung/Frage“ wird die Beschaffenheit, das Merkmal, die Funktion u.a. wiedergegeben.
* In der Spalte „Kriterienart“ wird angegeben, ob es sich um eine Ausschlusskriterium (A) oder ein Kriterium mit Priorität (H= Hoch; N=Niedrig) oder ein Informationskriterium (I), handelt (s.o.).

## 4.1 Allgemein

|  |  |  |
| --- | --- | --- |
| **1. Kriteriengruppe Allgemein** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 1.1. | Der Softwarehersteller stellt zuverlässig sicher, dass das Projekt dauerhaft über die gesamte Projektlaufzeit unterstützt werden kann. | H |
| 1.2. | Der von AMEOS dargelegte Scope / Zeitplan der Implementierung kann von Anbieterseite realisiert werden (vgl. Anlage 3 Lastenheft vgl. 11. Projektablauf) | A |

## 4.2 Support

|  |  |  |
| --- | --- | --- |
| **2. Kriteriengruppe Support** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 2.1. | Montag bis Sonntag von 00:00 bis 24:00 Uhr inklusive der gesetzlichen Feiertage am Ort des Auftraggebers und Auftragnehmers wird wie folgt Support und Fernwartung geleistet, vorausgesetzt, dass die erforderliche Serverinfrastruktur und die Datenbankanbindung für die IAM-Dienste verfügbar ist: | A |
| 2.1.1. | Prio 1 (betriebsverhindernd) - Kernfunktionalität der Software nicht gegeben, betriebswirtschaftlich oder technisch sinnvoller Einsatz nicht möglich: Reaktionszeit von 4 Stunden, Wiederherstellung nach 4 Stunden | A |
| 2.1.2. | Prio 2 (betriebsbehindernd) - Kernfunktionalität der Software gegeben; wesentlicher Fehler, der die Nutzung wesentlich erschwert: Reaktionszeit von 8 Stunden, Wiederherstellung nach 12 Stunden | A |
| 2.1.3. | Prio 3 - Andere Störungen: Reaktionszeit von 24 Stunden, Wiederherstellung nach 120 Stunden | A |
| 2.1.4. | Telefonischer Support durch eine deutschsprachige und sachkundige Hotline gemäß obiger Servicezeiten | H |
| 2.1.5. | Gewährleistung vorgegebener Verfügbarkeiten (siehe Absatz 3.3 und 4.8) einschließlich deren Dokumentation | H |
| 2.2. | Ergänzung und Aktualisierung der Systemdokumentation und des Betriebshandbuchs bei relevanten Änderungen; zu liefern mindestens 8 Wochen vor der Umsetzung, um den AMEOS IT-Services Zeit für Tests und Anpassungen zu geben | H |
| 2.3. | Alle Supportfälle, Incidents und Service Requests müssen im Ticketsystem der AMEOS Gruppe dokumentiert werden. Die Integration von Ticketsystemen zwischen dem Auftraggeber und dem Auftragnehmer ist optional möglich. | N |
| 2.4. | Remote Services: Systemzugriffe von Seiten des Auftragnehmers erfolgen ausschließlich nach vorheriger Absprache und Autorisierung durch die Systemverwaltung des Auftraggebers. | H |
| 2.5. | Etwaige Datenbanken werden durch Sie als Dienstleister installiert, eingerichtet und betrieben. | H |
| 2.6. | Für die Installation werden temporäre lokale Administratorrechte gewährt. Supportfälle sind ohne Administratorenrechte über einen sogenannten Superuser möglich. Hierfür ist einmalig die Angabe der notwendigen Berechtigungen durch Sie erforderlich. Alle Änderungen bzw. Anpassungen sind zu dokumentieren. | H |

## 4.3 Schulung

|  |  |  |
| --- | --- | --- |
| **3. Kriteriengruppe Schulung** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 3.1. | Die detaillierte Installations-, System- und Anwenderdokumentation liegt zu Projektbeginn in deutscher Sprache vor. Sie wird während der Projektlaufzeit auf dem aktuellen Stand gehalten. | H |
| 3.2. | Auf Seiten des Auftraggebers erfolgt die 1st-Level-Systembetreuung und Administration durch einen technischen Mitarbeiter + Vertretung. Diese sind zu Beginn des Projektes durch den Auftragnehmer zu schulen, sowie es erforderlich ist, dass bei wesentlichen Neuerungen des Systems durch Updates eine wiederholte Schulung zu den Neuerungen erfolgt. | A |
| 3.3. | Darüber hinaus sollen diese Mitarbeiter geschult werden, um Anpassungen am System (insbesondere: Implementierung vergleichbarer Anwendungs-fälle) sowie Support vor Ort selbst vornehmen zu können. | A |
| 3.4. | Des Weiteren ist durch den Auftragnehmer ein Konzept für die Key-User-Schulungen vorzulegen. Im Rahmen des Schulungskonzeptes sind durch den Auftragsnehmer Schulungsmodule zu definieren, wobei Inhalt und Umfang aufgezeigt werden. | H |
| 3.5. | Schulungen sind in deutscher Sprache abzuhalten, Schulungsunterlagen sind im Angebotspreis enthalten und werden durch den Auftragnehmer zur Verfügung gestellt. | H |
| 3.6. | Die Schulungen der Mitarbeiter zu dem System sollen hauptsächlich über ein E-Learning Portal stattfinden. Um dies zu ermöglichen, muss uns der Anbieter Lerncontent zur Verfügung stellen, welcher auf der AMEOS-eigenen Moodle-Plattform lauffähig ist. Typische Lernformate können sein: AICC, IMS. Idealerweise bietet der Anbieter Lernformate in SCORM 1.2 an. Alternativ können Exporte aus anderen Autorensystemen wie z.B. Articulate und Adobe-Produkte integriert werden. | H |

## 4.4 Ergänzungen

|  |  |  |
| --- | --- | --- |
| **4. Kriteriengruppe Ergänzungen** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 4.1. | Wie lange wird beabsichtigt, die Software in der jetzigen Form weiterzuentwickeln? | I |
| 4.2. | In welcher Form und in welchem Umfang erfolgen kritische und reguläre Updates sowie Major-Release-Wechsel der bereitgestellten Plattform? | I |
| 4.3. | Welche zukünftigen funktionalen und technologischen Erweiterungen des Produktes sind vorgesehen? | I |
| 4.4. | Wie weit wird der Auftraggeber in die Release-Planung mit einbezogen? | I |
| 4.5. | Welche Regelungen zu Updates, Upgrades und Lizenzverlängerungen bestehen? | I |
| 4.6. | Welche Skalierbarkeit besteht im Zusammenhang mit steigenden Nutzerzahlen oder wachsenden Datenmengen? | I |

## 4.5 Datensicherheit / Rechtekonzept

|  |  |  |
| --- | --- | --- |
| **5. Kriteriengruppe Datensicherheit/Rechtekonzept** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 5.1. | In dem IAM-System muss ein differenziertes Rollen- und Berechtigungskonzept möglich sein. Dabei sollte mindestens zwischen Administrator und MA der AMEOS IT-Services, MA der lokalen und zentralen HR-Abteilungen und MA der AMEOS Standorte unterschieden werden können. Die Dokumentation der Berechtigungen muss bei Produktivsetzung als Berechtigungskonzept übergeben werden. | A |
| 5.2. | Anmelden:   * über Single Sign On (SSO) * über Angabe von Windows Benutzernamen (AD) und Passwort. | A |
| 5.3. | Abmelden: Der Benutzer kann das System nur nutzen, wenn er registriert und angemeldet ist. Dies gilt somit für alle nachfolgenden Funktionen. Die Kennung des Mitarbeiters wird nach einem festgelegten Zeitrahmen ohne Interaktion automatisch geschlossen. | N |
| 5.4. | Das System entspricht allen gesetzlichen Anforderungen und branchenspezifischen Regularien im Geltungsbereich der EU, insbesondere von Deutschland und Österreich sowie der Schweiz. | A |
| 5.5. | Maßnahmen zur Gewährleistung der Daten- und Informationssicherheit müssen nach dem jeweiligen Stand der Technik durchgehend berücksichtigt sein und entsprechen den gültigen Datenschutzstandards der EU, insbesondere von Deutschland, Österreich sowie der Schweiz. | A |
| 5.6. | Zugriffsberechtigungen müssen dem Personal zugewiesen werden, inkl. Fach- und Stationszuordnung. Zugriffsberechtigungen sollen auch für Fremdpersonal (Anwender ohne User im LoGA HR-System) möglich sein. | A |
| 5.7. | Datensicherung und -austausch erfolgen verschlüsselt mit dem jeweils sichersten Standard nach dem aktuellen Stand der Technik. | H |

## 4.6 Leistungsanforderungen

|  |  |  |
| --- | --- | --- |
| **6. Kriteriengruppe Leistungsanforderungen** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 6.1. | Das IAM-System wird die folgenden Eintrittsprozesse (OnBoarding) unterstützen:  6.1.1. Eintritt neuer AMEOS-interner Mitarbeiter durch Trigger aus dem HR-System LoGA HR  6.1.2. Eintritt externer Mitarbeiter ohne LoGA HR über ein Web-Portal im IAM  6.1.3. Wiedereintritt pausierender Mitarbeiter | A |
| 6.2. | Das IAM-System wird die folgenden Anpassungen während des gesamten Mitarbeiterzyklus eines AMEOS-internen Mitarbeiters unterstützen:  6.2.1. Namensänderungen  6.2.2. Abteilungswechsel  6.2.3. Rollenwechsel, Beförderung, Herabstufung  6.2.4. Änderungen der Qualifikation  6.2.5. Unterbrechungen im Arbeitsverhältnis | A |
| 6.3. | Das IAM System wird folgende Austrittsprozesse (OffBoarding) unterstützen:  6.3.1. geplantes Ausscheiden eines Mitarbeiters getriggert durch LoGA HR  6.3.2. ungeplantes Ausscheiden mit sofortiger Wirkung per IAM-Applikation | A |
| 6.4. | Prozesse, die nicht vollintegrierbar und automatisierbar sind, müssen vor Inbetriebnahme des IAM komplett aufgenommen und dokumentiert sein. Diese können durch manuelle Aufgaben per E-Mail an den Service Desk (SD) gesendet werden. Eine positive Abschlussantwort per Mail vom SD lässt den Prozess im IAM fortführen. Bei negativer Rückmeldung zweigt der gestartete IAM-Prozess in die Fehlerbehandlung ab. | A |
| 6.5. | Jede genehmigende Person kann eigene offene und abgeschossene Aufgaben im IAM-System einsehen. | H |
| 6.6. | Anpassungen für Genehmigungsprozesse sind auf einfache Weise auch von Nicht-IT-Mitarbeitern durchführbar. Siehe Lastenheft Ziffer 6 Soll-Zustand. | A |
| 6.7. | Privileged Access Management (PAM) für befristete und zeitgesteuerte Admin-Zugänge wird vom IAM-Produkt unterstützt und in den Lizenzkosten im Preisblatt mit ausgewiesen. Es geht hier um die Steuerung von privilegierten Berechtigungen und Accounts.  Mengengerüst:  Zielsystem: 1000 Server, 2500 FAT-Clients  Anzahl User: 1500 privilegierte Accounts | H |
| 6.8. | Im Preisblatt Anlage 5 und im Pflichtenheft in Form des Technischen Konzeptes (Anlage 3 Ziffer 8) sind alle erforderlichen Schnittstellen gemäß Absatz „5.3.2 Schnittstellen und Kompatibilität“ aufzuführen bzw. zu berücksichtigen, die keine AD-Anbindung vorweisen. | A |

## 4.7 Systemarchitektur

|  |  |  |
| --- | --- | --- |
| **7. Kriteriengruppe Systemarchitektur** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 7.1. | Das System soll als On-Premise-Lösung angeboten werden. | A |
| 7.2. | Systemsprache: Das System ist mindestens in deutscher Sprache verfügbar. | A |
| 7.3. | Das System kann in mehreren Sprachen (insbesondere Englisch) verfügbar sein. | N |
| 7.4. | Das System muss mit der LoGA HR-Anwendung der P&I AG in Wiesbaden (Hosting als SaaS) per csv-Textdateischnittstelle ereignisgesteuert kommunizieren können. (LoGA -> IAM) | A |
| 7.5. | Der Anbieter sollte Kenntnisse für die Integration von LoGA HR haben. | H |
| 7.6. | Der Anbieter sollte Kenntnisse für die Integration der Dienstplansoftware Polypoint PEP haben. | H |
| 7.7. | Der Anbieter sollte Kenntnisse für die Integration der Dienstplansoftware Clinic Planner haben. | H |
| 7.8. | Der Anbieter sollte Erfahrung für die Integration der Dienstplansoftware SPExpert haben. | H |
| 7.9. | Die Systemarchitektur muss kompatibel zu den im technischen Konzept (Anlage 3) aufgeführten Rahmenbedingen (siehe Ziffer 3 „AMEOS IT-Architektur“) sein. | A |

## 4.8 Verfügbarkeit des Systems

|  |  |  |
| --- | --- | --- |
| **8. Kriteriengruppe Verfügbarkeit des Systems** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 8.1. | Angabe der maximal garantierten Verfügbarkeit in % | H |
| 8.2. | Angabe der maximalen Ausfallzeit pro Jahr in Stunden | H |

## 4.9 Schnittstellen / Kompatibilität

|  |  |  |
| --- | --- | --- |
| **9. Kriteriengruppe Schnittstellen / Kompatibilität** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 9.1. | Um ein hohes Maß an Interoperabilität zu erreichen, muss die Lösung international anerkannte technische, syntaktische und semantische Standards unterstützen:  1.Technische Standards:   * ISO/IEC 27001:2013 - Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen * ISO/IEC 20000-1:2018 - Informationstechnologie - Servicemanagement - Teil 1: Anforderungen an ein Servicemanagementsystem * ISO/IEC 9001:2015 - Qualitätsmanagement - Anforderungen   2.Syntaktische Standards:   * XML (Extensible Markup Language) - Ein Standard für die Kodierung von Dokumenten in einem Format, das von verschiedenen Systemen gelesen und verarbeitet werden kann * JSON (JavaScript Object Notation) - Ein leichtgewichtiges Datenaustauschformat, das von vielen Programmiersprachen unterstützt wird * HTML (Hypertext Markup Language) - Ein Standard für die Erstellung von Webseiten   3.Semantische Standards:   * RDF (Ressource Description Framework) - Ein Framework für die Beschreibung von Ressourcen im Web, das die Semantik von Daten modelliert * OWL (Web Ontology Language) - Eine Sprache zur formalen Beschreibung von Wissen im Web * SKOS (Simple Knowledge Organisation System) - Ein Standard für die Organisation von Wissen und die Erstellung von Thesauri und Vokabularen | N |
| 9.2. | Das IAM-System sollte die Konnektivität zu den in Kapitel 5.3.2. gelisteten Systemen unterstützen. Nicht unterstützbare Systeme sind im Kriterienkatalog Anlage 4 in den Bemerkungen zu benennen. | I |
| 9.3. | Das IAM-System muss im Bereich der Nicht-AD-fähigen Applikationen kompatibel zur bereits innerhalb der AMEOS Gruppe eingesetzten SSO Plattform sein. (siehe Anlage 3 „Technisches Konzept“ Ziffer 3 „AMEOS IT-Architektur“) | H |
| 9.4. | Die Schnittstellen in Kapitel 5.3.2 sind im Angebot als einzelne Positionen aufzuführen. | I |

## 4.10 Systemanforderungen

Die Anlage 3 zur Ausschreibung, „Technisches Konzept“, umfasst alle IT spezifischen Rahmenbedingungen und Anforderungen. Alle im technischen Konzept abgefragten Informationen, sind in dieser Anlage zu hinterlegen. Das technische Konzept dient zur Evaluierung der Systemarchitektur und ist die Grundlage der technischen Umsetzung im Verlauf des Einführungsprojektes.

|  |  |  |
| --- | --- | --- |
| **10. Kriteriengruppe Systemanforderungen** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 10.1. | Es ist in einem Betriebshandbuch nach AMEOS-Vorlage darzustellen, wie das System nach Abschluss des Projekts betrieben und supportet wird. | H |
| 10.2. | Neben dem Produktivsystem ist vom Auftragnehmer auch ein Testsystem zu implementieren und auszuliefern. | N |
| 10.3. | Das Testsystem ist auf einem vom Produktivsystem getrennten Server-system zu implementieren. | N |
| 10.4. | Prozesse können per Schnittstelle oder Export/Import vom Testsystem ins produktive System als Paket übertragen werden. | H |
| 10.5. | Das System muss mandantenfähig sein. Die Mandantenfähigkeit muss auf unterschiedliche Länder anwendbar sein. Auf nicht mandantenfähige Applikationen ist ausdrücklich hinzuweisen. | A |
| 10.6. | Die zentral eingesetzte Software muss in die IT-Architektur der AMEOS Gruppe gemäß dem technischen Konzept Anlage 3 integrierbar und insbesondere virtualisiert unter VMware betreibbar sein. | A |
| 10.7. | Das IAM-System muss auf neue Standorte erweiterbar sein und sollte durch ein Rollen- und Berechtigungskonzept (gemäß DSGVO) ergänzt werden. | A |
| 10.8. | Es werden für Berechtigungsvergaben an Verzeichnissen und Applikationen heterogene Berechtigungsstrukturen in verschiedenen Standorten bzw. Sub-Active-Directories unterstützt. | A |
| 10.9. | Das System verfügt über eine Backup-Funktion (Backup der Konfiguration und Audittrails). | H |
| 10.10. | Die Benutzeroberfläche muss an das Corporate Design von AMEOS anpassbar sein. | N |
| 10.11 | Oracle Datenbanken sind ausschließlich nach vorheriger Absprache anzubieten. | I |

## 4.11 Softwarepflege

|  |  |  |
| --- | --- | --- |
| **11. Kriteriengruppe Softwarepflege** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 11.1. | Die Lieferung von Updates und Upgrades (neue Programmversionen mit erweiterter Funktionalität innerhalb des erworbenen Lizenzumfangs) einschließlich deren Installation erfolgt grundsätzlich im Rahmen der vereinbarten Laufzeit und des Wartungsvertrages, ohne Extrakosten. | H |
| 11.2. | Der Auftragnehmer wird das Gesamtsystem ab Auftragsvergabe für mindestens fünf Jahre weiter pflegen. | H |

## 4.12 Anwendungsfall

Im Rahmen der Ausschreibung möchten wir Sie bitten, uns Unterlagen einer Produktpräsentation in Form eines Anwendungsfalls als Anhang zum Angebot mit zu übersenden. Stellen Sie uns die Produktpräsentation bitte als Live- Demonstration in einem Video zur Verfügung.

|  |  |  |
| --- | --- | --- |
| **12. Kriteriengruppe Anwendungsfall** | |  |
| **Kriterien-Nr.** | **Anforderung / Frage** | **Kriterienart** |
| 12.1. | Ein zukünftiger Mitarbeiter hat nach erfolgreichem Bewerbungsgespräch seinen Arbeitsvertrag erhalten und das Abrechnungssystem sendet den Trigger zum OnBoarding an das IAM-System. Es genügt, die Funktionsweise (z.B. Simulation des Triggers in Richtung IAM System) darzustellen und mit einer Testdatei aussagekräftig die Erzeugung einer neuen Identität zu belegen mit folgenden Mindestdaten:   * Name, Vorname, Titel, eindeutige Personalnummer, * Gültigkeit (Eintritt und Austritt), primärer Einsatzort   Bitte stellen Sie den Prozess dar, wie das IAM-System   * den Benutzerprinzipalname UPN des neuen Mitarbeiters erzeugt Dazu kann das IAM-System mit Übersetzungstabellen arbeiten und Standortinformationen des primären Einsatzortes in Standortkürzen verwandeln. Z.B. kkvnnn oder falls dieser UPN bereits besteht, auch kkvvvn. k = Kürzel, v = Vorname, n = Nachname * den Genehmigungsprozess abbildet * dem Account Standardrollen seiner neuen Abteilung zugewiesen werden * für den Account ein Exchange-Postfach angelegt wird.   Stellen Sie im weiteren Verlauf dar, auch simuliert, wie das IAM-System   * mit einem Dienstplansystem korrespondiert. * einen Abteilungswechsel prozessual abbildet * auf Namenswechsel durch Heirat, Scheidung von einem Abrechnungssystem reagiert * Arbeitsunterbrechungen, z.B. Sabatical, Elternzeit, längerfristige Erkrankungen flexibel verarbeitet. * das Ausscheiden eines Mitarbeiters erfolgt.   Stellen Sie außerdem dar,   * welche Felder Sie in der Schnittstelle von Abrechnungssystemen und von Dienstplansystemen erwarten. * wie das IAM-System an weitere Systeme angebunden werden kann. * welche Audit- und Reportmöglichkeiten bestehen.   Die Präsentation sollte nicht länger als 45 Minuten benötigen. | A |

# Produktanforderungen

## 5.1 Funktionale Anforderungen

Das IAM System muss in der Lage sein, entsprechend des AMEOS Mitarbeiterzyklus vordefinierte Maßnahmen automatisiert durchzuführen. Der Mitarbeiterzyklus besteht aus Eintritt, Veränderung und Austritt. Für jeden der drei Zustände sind unterschiedliche Maßnahmen zu ergreifen, die hier aufgeführt werden. Das IAM muss dabei folgende Aufgaben durchführen.

### Eintritt

Wird ein Mitarbeiter im Bewerbermanagement LoGA HR Bewerber 3 als eingestellt gekennzeichnet, übernimmt das IAM die Stammdaten und legt für den Mitarbeiter die seiner Rolle definierten funktionsspezifischen Rollen und notwendigen IT Ressourcen an (AD User, AD Mitgliedschaften, Exchange Postfach, i.s.h.med Zugriff, …). Die Freigabe des AD-Accounts wird zeitlich synchronisiert mit dem Eintrittsdatum.

Externe Mitarbeiter und administrative Konten werden direkt im Self-Service-Portal des IAM angelegt. Die Genehmigung muss mindestens zweistufig möglich sein mit frei zu definierenden Stufen.

### Berechtigungsrelevante Veränderung

Berechtigungsverändernde Vorgänge werden bei AMEOS-intern Mitarbeitenden angestoßen durch geplante Funktions-, Abteilungs- oder Standortwechsel im LoGA HR. Kurzfristige Abteilungswechsel werden auch durch die Personaleinsatzplanung „Dienstplan 3“, Polypoint PEP, Clinic Planner und SPExpert initiiert. AMEOS-externe Dienstleister werden von den internen Ansprechpartnern im IAM System angelegt und in einem mindestens zweistufigen Genehmigungsverfahren freigegeben.

### Nicht-Berechtigungsrelevante Veränderung

Namensänderungen an Identitäten werden aus LoGA HR übernommen und an Applikationen und das Active Directory weitergeleitet. Änderungen an persönlichen Daten, die im IAM vom Mitarbeitenden per Self-Service eingegeben werden, lösen Prozesse inklusive Genehmigungsverfahren aus, mit denen die Daten dann ins LoGA HR zurückgespiegelt werden.

### Austritt

Austritte von Mitarbeitenden werden durch die HR-Abteilung initiiert. Es wird im HR System LoGA HR der Austritt zeitlich festgelegt. Entsprechend dieser Änderung muss das IAM System bestehende Zugänge ab dem definierten Zeitpunkt sperren, deaktivieren bzw. ein entsprechendes Accountablaufdatum setzen. Das LoGA HR teilt dem IAM System mit, ab wann die Zugänge des Mitarbeitenden gesperrt sein müssen.

Zusätzlich sollte die Möglichkeit bestehen, einen Sofortaustritt auch im IAM-System zu veranlassen. Kommt es zu einer umgehenden Beendigung des Arbeitsverhältnisses, muss es möglich sein, alle vorhandenen Zugänge des Mitarbeiters zu sperren.

Bei Austritten dürfen keine verwaisten Rollenverantwortlichkeiten, Vorgesetzten- und Vertretungsregelungen entstehen.

### Pausen und ruhende Arbeitsverhältnisse

Unterbrechungen werden wie temporäre Austritte behandelt. Für diesen Zeitraum werden ebenfalls Zugänge gesperrt, alle Berechtigungen entzogen und Rollenverantwortlichkeiten per Workflow an Vertreter oder Vorgesetzte übertragen.

### Nutzer ohne Active Directory Account

Jeder Mitarbeiter, der Zugriff zu Applikationen ohne Active Directory und LDAP-Anbindung erhalten soll, benötigt dennoch mindestens einen eigenen AD-Account und einen Vorgesetzten für die hierarchische Freigabe. Funktionsbezogene Zugänge wie z.B. Stationsaccounts werden in den vorbereitenden Maßnahmen durch personalisierte Accounts abgelöst. Des Weiteren werden multiple Accounts über die Gesellschaften hinweg konsolidiert, sodass für jeden Mitarbeiter nur noch eine Identität über alle Gesellschaften hinweg existiert.

### Digitaler „Laufzettel“

Das IAM System soll einen Digitalen Laufzettel abbilden können. Wird ein Mitarbeiter mit Arbeitsmitteln ausgestattet, muss die Ausgabe und der Empfang der Mittel digital quittiert (hierarchischer Freigabeworkflow) werden. Dies muss auch für die Rückgabe der Mittel entsprechend abgebildet werden. Es müssen zu den Arbeitsmitteln der Hersteller und das Modell und ggfs. Seriennummer, Rufnummern und IMEI-Nummern erfasst werden können. Es muss ein Export der Arbeitsmittel inkl. des nutzenden Mitarbeiters in die CMDB möglich sein.

### Synchronisationszeitpunkt

Um die geplanten Lohnabrechnungsläufe nicht zu beeinträchtigen, ist es wichtig, dass das IAM System nicht während der Nachtstunden intensiv auf das HR-System zugreift. Im Zeitraum von 01:00 – 05:00 Uhr darf das IAM nicht auf die im LoGA HR hinterlegten Daten zugreifen.

## Nichtfunktionale Anforderungen

Da das System unter Umständen personenbezogene Daten speichert und verarbeitet, muss es den gängigen Datenschutzkriterien entsprechen: DSGVO; BSI B3S; ISO 27001; § 75c SGB V.

Erweiterungen oder Anpassungen an dem IAM System oder den Schnittstellen müssen, in Zuhilfenahme des Herstellers, implementierbar sein.

Das IAM System hat weitestgehend selbsterklärend zu bedienen zu sein und den Anwender durch Hilfestellungen, Tooltips oder durch weitergehende Hilfefunktionen zu unterstützen.

Das System muss barrierefrei sein.

## Technische Anforderungen

### 5.3.1 Allgemeine Anforderungen

Es muss die Möglichkeit bieten zeitliche Auswertungen über Vergaben, Entzug und den IST Stand von Benutzerrechten zu geben (Reporting inklusive Archivfunktion in Form von revisionssicherem Logging und revisionssicherer Dokumentation).

Es muss Schnittstellen in die von AMEOS betriebenen Softwaresysteme bieten (siehe hier im Lastenheft Ziffer 5.3.2 „Schnittstellen und Kompatibilität“) oder soweit anpassbar sein, dass Schnittstellen dafür entwickelt, hinzugefügt und angepasst werden können.

Nicht durch IAM ansprechbare Systeme müssen über Zustellung einer manuellen Aufgabe (Support-Ticket) an den AMEOS IT-Service Desk in einem Workflow administriert werden können.

Für den Zugriff auf das IAM System muss ein Rollenmodell (RBAC) implementierbar sein.

Jede Rolle soll mindestens von zwei Personen verantwortet werden, das ist bei der Einrichtung einer Rolle zu garantieren, Rollen mit nur einem Verantwortlichen müssen in einem monatlichen / wöchentlichen Report sichtbar werden.

Das IAM muss über Browser und ohne zusätzliche Installationen oder Konfigurationen auf Clients betreibbar sein~~.~~

Das IAM muss in der Lage sein, einen E-Mail-Server verschlüsselt zu kontaktieren, um Emails zu versenden bzw. zu empfangen. Es bedarf einer authentifizierten Anmeldung zum Versand von E-Mails auf unserer Exchange Infrastruktur.

Aus Antworten von Nutzern und Rückmeldungen des Ticket-Systems müssen Workflows fortgesetzt werden können. Hierzu müssen eingehende Mails den Benutzern eineindeutig zuordnet werden und auf zu definierende Schlüsselwörter hin ausgewertet werden. Diese Schlüsselwörter oder Phrasen stoßen die Workflows an.

Personenbezogene Daten müssen nach aktuellem Stand der Technik maximal verschlüsselt werden. Sowohl bei der Speicherung, als auch beim Transport.

Die Synchronisation der Identitäten muss zeitgesteuert durchgeführt werden und darf andere Systeme nicht in ihrer Funktion stören oder unterbrechen.

Es ist in der Dokumentation zu beschreiben, wie das AMEOS IT-Personal Updates einspielen, sowie Wartungen und Notfallwiederherstellungen durchführen kann.

Die Vorlage des AMEOS IT-Betriebshandbuches ist vollständig auszufüllen.

### 5.3.2 Schnittstellen und Kompatibilität

Das IAM greift in betriebene Prozesse und Systeme verwaltend ein, Schnittstellen sind somit von besonderer Bedeutung. Im Optimalfall bietet das IAM bereits bei Auslieferung eine hohe Anzahl von verfügbaren Schnittstellen. Zusätzlich muss die Implementierung weiterer Schnittstellen möglich sein. Schnittstellen müssen vollständig dokumentiert und getestet werden. Die Dokumentation sollte eine Skizze der Kommunikationswege enthalten.

Der initiale Scope des Projektes umfasst die Koppelung des Microsoft Active Directory und des HR-Systems LoGA HR.

Zusätzlich sollte es optional möglich sein, die folgenden Systeme für eine Berechtigungsvergabe an das IAM anzubinden. Bitte geben Sie im Angebot pro System an, ob eine Anbindung zu welchen Kosten möglich ist, differenziert nach AD- und Non-AD-Fähigkeit:

|  |  |  |
| --- | --- | --- |
| System | Beschreibung | Typ |
| LoGA HR | Lohn und Gehaltsabrechnung | SaaS Dienst |
| SAP | ERP | On-Premise zentral |
| SAP Cerner i.s.h.med | KIS | On-Premise zentral |
| Microsoft Exchange | Emailsystem | On-Premise zentral / dezentral |
| Dienstplansoftware  Polypoint PEP | Dienstplan und Ressourcenmanagement | On-Premise zentral / dezentral |
| Qlik View | Reporting | On-Premise zentral |
| PACS-Sectra | RIS/PACS | On-Premise dezentral |
| RIS-GE | RIS/PACS | On-Premise dezentral |
| Labuniq | Labor | On-Premise zentral |
| Medlinq | Speiseversorgung | On-Premise zentral |
| Maris | Digitales Diktat | On-Premise dezentral |
| xSuite | Rechnungsverarbeitung | On-Premise zentral |
| Doctolib | Online Terminplanung | On-Premise zentral |
| ERPath | Notaufnahme | On-Premise zentral |
| GeDoWin | Geburtendokumentation | On-Premise zentral |
| Medlinq | Anästhesie | On-Premise zentral |
| 3M QS Med Suite | Qualitätssicherung | On-Premise zentral |
| 3M 360 Encompass | Kodierung | On-Premise zentral |
| 3M MD Management | Medizinischer Dienst | On-Premise zentral |
| Nuance | Spracherkennung | On-Premise zentral |
| eConsent | Thieme Aufklärung | On-Premise zentral |
| SSO Imprivata | Single Sign On | On-Premise zentral |
| Celsius 37 | Tumor-Dokumentation | On-Premise zentral |
| Pflegeplatzmanager | Überleitungsmanagement | On-Premise zentral |
| OTRIS DMS | Dokumentenlenkungssystem | On-Premise zentral |
| OTRIS Contract | Vertragsmanagement | On-Premise zentral |
| Medical Office | AIS – Arztinformationssystem | On-Premise zentral / dezentral |
| Reha.Complete | Patientenverwaltung | On-Premise zentral |
| KIX | IT-Ticketverwaltung | On-Premise zentral |
| QCare | Elektronische Dokumentation | On-Premise zentral |
| Nexus | Geburtendokumentation | On-Premise zentral |

### 5.3.3 Systemanforderungen - IT

Die Systemanforderungen sind im Technischen Konzept (Anlage 3) beschrieben.

### 5.3.4 Unterlagen die mit Inbetriebnahme zur Verfügung zu stellen sind

• Rollenbasierendes Berechtigungskonzept – gem. der zum Zeitpunkt der Ausschreibung bestehenden gesetzlichen Anforderungen (auf Userebene).

• Betriebshandbuch

• Dokumentation der Systemkonfiguration und -installation (IQ)

• Wartungs- und Wiederherstellungsanleitung für die AMEOS IT-Services

# Soll – Zustand

Angestrebt ist, dass IAM als On-Premise Lösung zu betreiben. Für die On-Premise Installation müssen die unter „Ziffer 4.10 Systemanforderungen“ aufgeführten Konfigurationen als zentral bereitgestellte VM verwendet werden. Das Lizenzmodell muss von Auftragnehmer im technischen Konzept (Anlage 3) beschrieben werden. Entsprechend erforderliche Firewall-Freischaltungen und Kommunikationsverbindungen sind im technischen Konzept anzugeben.

Wie in Punkt 5.3.2. beschrieben, soll vom IAM System aus eine Schnittstellenverbindung zu den zu verwaltenden Systemen bestehen. Als zentraler Punkt werden Rollen, Berechtigungen, Logiken, Workflows, etc. zentral im IAM verwaltet. Anhand der vorher definierten und festgelegten Parameter unternimmt das IAM die auszuführenden Schritte. Ziel ist die weitergehende Automatisierung des Mitarbeiterlebenszyklus. Da sich Unternehmensprozesse immer wieder ändern, muss auch das IAM möglichst flexibel sein. Anpassungen an geänderte Geschäftsprozesse oder Abläufe sollen möglichst einfach und schnell im IAM abgebildet werden können. Ziel ist es, dass dies auch von „Nicht-IT-Personal“ vorgenommen werden kann. (siehe Kriterienkatalog Anlage 4 Ziffer 6.6)

# Zukünftige Erweiterungen

Da die AMEOS Gruppe kontinuierlich wächst und somit auch mehr Mitarbeitende beschäftigt, muss auch das IAM System mitwachsen. Perspektivisch werden weitere Systeme, Domänen und Standorte angebunden werden. Weitere Schnittstellenimplementierungen zu verwalteten Systemen werden hinzukommen. Dies muss IAM seitig abbildbar sein.

Entsprechende Lizenzen müssen erweiterbar oder reduzierbar sein.

# Schulungen / Dokumentation

Eine Dokumentation des IAM Systems wird vorausgesetzt. Diese kann online oder per Überreichen der Dokumentation in digitaler Form abgebildet sein.

Während der Bereitstellung, Einrichtung und Anpassung des IAM Systems müssen über die vorgenommenen Arbeiten Protokolle verfasst werden. Diese dienen als Grundlage des Betriebshandbuches.

* Die detaillierte Installations-, System- und Anwenderdokumentation liegt in deutscher Sprache vor. Sie wird während der Projektlaufzeit auf dem aktuellen Stand gehalten.
* Auf Seiten des Auftraggebers erfolgt die 1st-Level-Systembetreuung und Administration durch einen technischen Mitarbeiter + Vertretung. Diese sind zu Beginn des Projektes durch den Auftragnehmer zu schulen, sowie es erforderlich ist, dass bei wesentlichen Neuerungen des Systems durch Updates eine wiederholte Schulung zu den Neuerungen erfolgt.
* Darüber hinaus sollen diese Mitarbeiter geschult werden, Anpassungen am System (insbesondere: Implementierung vergleichbarer Anwendungsfälle) sowie Support vor Ort selbst vornehmen zu können.
* Des Weiteren ist durch den Auftragnehmer ein Konzept für die Key-User-Schulungen vorzulegen. Im Rahmen des Schulungskonzeptes sind durch den Auftragsnehmer Schulungsmodule zu definieren, wobei Inhalt und Umfang aufgezeigt werden.
* Schulungen sind in deutscher Sprache abzuhalten, Schulungsunterlagen sind im Angebotspreis enthalten und werden durch den Auftragnehmer zur Verfügung gestellt.
* Die Schulungen der Mitarbeiter zu dem System sollen hauptsächlich über ein E-Learning Portal stattfinden. Um dies zu ermöglichen, muss uns der Anbieter Lerncontent zur Verfügung stellen, welcher auf der AMEOS-eigenen Moodle-Plattform lauffähig ist. Typische Lernformate können sein: AICC, IMS. Idealerweise bietet der Anbieter Lernformate in SCORM 1.2 an. Alternativ können Exporte aus anderen Autorensystemen wie z.B. Articulate und Adobe-Produkte integriert werden.

# Service / Support / Updates

Im Umfang des Angebotes des Auftragnehmers soll ein Angebot für einen Wartungsvertrag enthalten sein. In diesem Rahmen sollen Kosten und Aufwände für Updates, Supportfälle, Unterstützungsleistungen aufgeführt werden. Idealerweise geschieht dies über eine Fix-Pauschale. Auch ist zu beschreiben welche zeitlichen und finanziellen Aufwände für das Erstellen von zusätzlichen Schnittstellen, differenziert nach AD- und Non-AD-Fähigkeit entstehen.

In jedem der Bereiche werden vom Auftragnehmer Mindestqualitäten gefordert, die im Folgenden als Service Level Agreement (SLA) bezeichnet werden. SLAs dienen dazu, Bedingungen und Kriterien der Leistungserbringung zu definieren. Beispiele für solche SLAs sind:

• Verfügbarkeiten von Services

• Erreichbarkeitszeiten von Service-Geschäftsstellen und Hotlines

• Reaktionszeiten bis zum Beginn der Fehlerbehebung in Störfällen

• Wiederherstellungszeiten nach Systemausfällen

# Voraussichtliches Mengengerüst

Gegenwärtig existieren im AD Umfeld der AMEOS Gruppe ca. 12.500 aktive Benutzerkonten bei ca. 18.000 Mitarbeitenden (Stand Mai 2024).

In der finalen Ausbaustufe wird mind. diese Anzahl von Benutzern verwaltet werden müssen. Das Mengengerüst sollte flexibel sein, um sowohl das Wachstum als auch eine Anpassung an veränderte Bedingungen im Unternehmen zu ermöglichen und somit die dynamische Entwicklung der Organisation zu unterstützen.

# Projektablauf

## 11.1 Zeitrahmen

Das IAM System soll technisch bis 31.10.2024 mit Anbindung LoGA und AD implementiert sein. Danach findet bis 31.12.2024 die Abbildung des Mitarbeiterlebenszyklus der AMEOS Gruppe statt.

## 11.2 Geplanter Ablauf

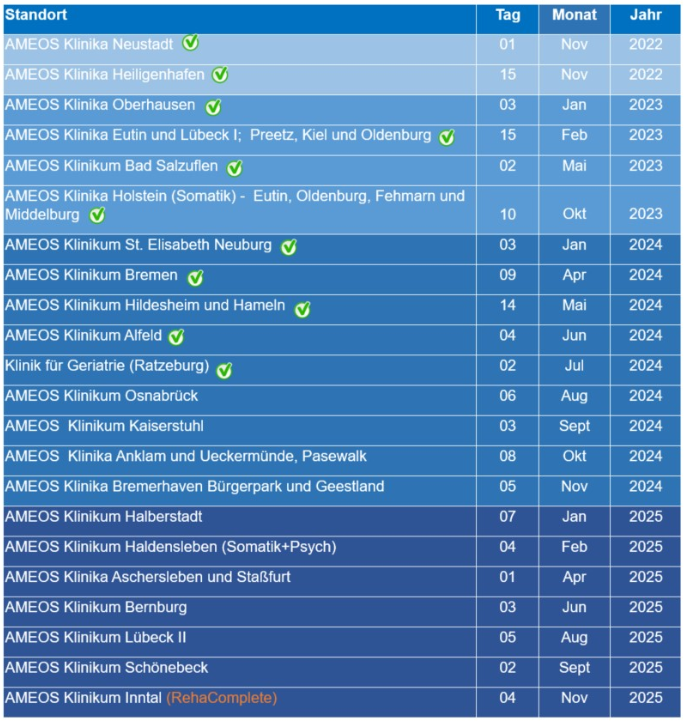
|  |  |  |
| --- | --- | --- |
| **Teilschritt** | **Beschreibung** | **Termin** |
| **Umsetzung** |  |  |
| Beginn | Projektstart | 01.10.2024 |
| Technische Verfügbarkeit | On-Premise Installation sowie Exchange- und AD-Anbindung abgeschlossen | 31.10.2024 |
| Operative Verfügbarkeit | LoGA HR -> IAM -> AD | 31.10.2024 |
| Operative Verfügbarkeit | KHZG Standorte mit einem GoLive Termin bis 31.12.2024 | 31.12.2024 |
| Operative Verfügbarkeit | KHZG Standorte mit einem GoLive Datum im Zeitraum 01.01.2025 bis 31.12.2025 | entsprechend Rolloutplan KHZG |
| Operative Verfügbarkeit | Alle nicht KHZG-relevanten Standorte | 31.12.2026 |

## 11.3 IAM Schnittstellen und Funktionalitäten Mindestumfang:

|  |  |  |
| --- | --- | --- |
| 1 | LoGA HR-> IAM | Mitarbeiter-Lebenszyklus (OnBoarding, Änderungen, Pausierungen, OffBoarding) |
| 2 | IAM -> AD | Benutzeranlage, Änderungen, Account-Freigabe, Account-Sperrung |
| 2a | IAM -> Exchange | Neue Exchange Mailbox |
| 3 | IT -> IAM Konfiguration | Erstellung Standard Profile nach Berufsbezeichnung / Funktion |
| 4 | IT -> IAM Konfiguration | Prozessdefinition Berechtigungsvergaben (Shares, Applikationen) |
| 5 | User -> IAM | Beantragung erweiterte Berechtigungen |
| 6 | IAM <-> Vorgesetzte | Genehmigungsverfahren (disziplinarisch) |
| 7 | IAM <-> DataOwner | Genehmigungsverfahren (Sharefreigaben) |
| 8 | IAM <-> Abteilungsleiter | Genehmigungsverfahren (Fachbereiche) |
| 9 | IAM -> AD | Abbildung der Rollen für die Standard Profile |
| 10 | IAM -> AD | Zuordnung der User zu den Rollen |

## 11.4 Rolloutplan des KHZG-Programms

… der Digitalen Transformation für die AMEOS Gruppe (Stand 01.August 2024)



# 12 Hinweis

Dem EVB-IT-Systemliefervertrag wird die durch den Auftragnehmer ausgefüllte Vorlage „Technische Konzept“ (Anlage 4 der Ausschreibung), als Ergänzung zum Pflichtenheft beigefügt.