

Leistungsbeschreibung

Einführung eines Identity- und Access-Management-Systems

Staatsbibliothek zu Berlin - Preußischer Kulturbesitz
IAM-System

Inhaltsverzeichnis

1	Einleitung	5
1.1	Hintergrund und Anlass.....	5
1.2	Zielsetzung	5
1.3	Systemlandschaft.....	6
1.4	Projektrahmen.....	6
2	Gegenstand der Leistung	7
2.1	Überblick.....	7
2.2	Funktionale Anforderungen	7
2.2.1	Benutzermanagement.....	7
2.2.2	E-Mail- und Exchange-Management	8
2.2.3	Verzeichnis- und Berechtigungsmanagement (File Server).....	8
2.2.4	Telefonmanagement (Cisco Callmanager)	8
2.2.5	Druckermanagement.....	9
2.2.6	Reporting	9
2.2.7	Self-Service-Portal	9
2.3	Abgrenzung – Nicht Gegenstand der Leistung.....	10
3	Anforderungen an den Auftragnehmer	10
3.1	Personalanforderungen.....	10
3.2	Projektdurchführung.....	10
3.3	Compliance- und Sicherheitsanforderungen	10
3.4	Dokumentation.....	11
3.5	Support, Wartung und Pflege	11
3.6	Exit Management	11
3.7	Ergänzende Dienstleistungen	12
4	Liefergegenstände und Ergebnisse	12
4.1	Zu liefernde Dokumente.....	12
4.2	Technische Liefergegenstände	12
4.3	Abnahme	12
5	Zeitplan und Meilensteine.....	13
5.1	Projektbeginn.....	13
5.2	Projektphasen und Meilensteine	13
5.3	Berichtswesen.....	14
6	Anforderungskatalog	26
6.1	Active Directory Muss-Anforderungen.....	26
6.2	Audit und Dokumentation Muss-Anforderungen	26
6.3	Berechtigungen Muss-Anforderungen.....	26
6.4	Fileserver Muss-Anforderungen	13
6.5	Microsoft Exchange Muss-Anforderungen.....	14
6.6	Microsoft 365 und Azure AD Muss-Anforderungen	14

6.7	OneDrive Muss-Anforderungen.....	15
6.8	Microsoft SharePoint Muss-Anforderungen.....	15
6.9	Passwort-Reset Muss-Anforderungen.....	15
6.10	PowerShell Muss-Anforderungen.....	15
6.11	Self Service Muss-Anforderungen.....	15
6.12	Support und Dokumentation Muss-Anforderungen.....	16
6.13	Systemumgebung Muss-Anforderungen	16
6.14	Third-Party-Integrationen Muss-Anforderungen	16
6.15	User Lifecycle und Profile Muss-Anforderungen.....	16
6.16	Workflows Muss-Anforderungen	17
6.17	Rezertifizierung Muss-Anforderungen	17
6.18	Technische Umgebung und Hosting Muss-Anforderungen.....	17
6.19	Schnittstellen (Basisfunktionen) Muss-Anforderungen	17
6.20	Anpassbarkeit (No-Code-Plattform) Muss-Anforderungen	18
6.21	Reporting Muss-Anforderungen	18
6.22	Rechte- und Rollenmanagement (Plattform) Muss-Anforderungen	18
6.23	E-Mail-Versand Muss-Anforderungen	18
6.24	Benutzeroberfläche (Interface) Muss-Anforderungen	19
6.25	Active Directory Wunsch-Anforderungen.....	19
6.26	Fileserver Wunsch-Anforderungen.....	19
6.27	Helpdesk-Integration Wunsch-Anforderungen.....	20
6.28	Microsoft Teams Wunsch-Anforderungen	20
6.29	Passwort-Reset Wunsch-Anforderungen	20
6.30	PowerShell Wunsch-Anforderungen	20
6.31	Self Service Wunsch-Anforderungen	20
6.32	Third-Party-Integrationen Wunsch-Anforderungen	20
6.33	Workflows Wunsch-Anforderungen	21
6.34	Rezertifizierung Wunsch-Anforderungen.....	21
6.35	Funktionstrennung (SOD) Wunsch-Anforderungen	21

1 Einleitung

1.1 Hintergrund und Anlass

Die Staatsbibliothek zu Berlin betreibt derzeit eine gewachsene IT-Infrastruktur zur Verwaltung von rund 3.500 Benutzerkonten über mehrere heterogenen Systeme hinweg. Das bestehende Identity- und Access-Management (IAM) genügt den aktuellen Anforderungen hinsichtlich Sicherheit, Automatisierung und zentraler Steuerbarkeit nicht mehr. Es besteht erheblicher Handlungsbedarf sowohl bei der Konsolidierung der Identitätsverwaltung als auch bei der Ablösung veralteter Prozesse und Systeme.

Leistungsgegenstand ist die Einführung einer modernen IAM-Lösung aus, die das bestehende System vollständig ablöst und einen einheitlichen, automatisierten Identity-Lifecycle für alle Benutzer und Berechtigungen gewährleistet.

1.2 Zielsetzung

Ziel des Vorhabens IAM-System ist die Implementierung und Inbetriebnahme einer leistungsfähigen IAM-Plattform, die folgende strategische Ziele erfüllt:

- Zentrale Identitätsverwaltung für alle Mitarbeiterinnen und Mitarbeiter der Behörde
- Automatisierung des vollständigen Benutzer-Lifecycles (Onboarding, Änderung, Offboarding)
- Konsolidierte Rechtevergabe nach dem Least-Privilege-Prinzip
- Nahtlose Integration in die bestehende und zukünftige IT-Systemlandschaft
- Erhöhung der IT-Sicherheit und Erfüllung behördlicher Compliance-Anforderungen (z. B. BSI-Grundschutz)

1.3 Systemlandschaft

Die IAM-Lösung ist in folgende Systeme der Behörde zu integrieren:

Kategorie	Systeme	Funktionsumfang
Verzeichnisdienste	Active Directory	Verwaltung von Nutzern, Gruppen und OUs; Multi-Domain-Unterstützung wünschenswert
Verzeichnisdienste	Azure Active Directory	Verwaltung von Nutzern und Lizenzzuweisungen
Datei- & Druckinfrastruktur	FileServer	Setzen und Prüfen von NTFS-Berechtigungen; optional: Speicherauslastung auslesen
Datei- & Druckinfrastruktur	Druckerserver	Erstellen und Verwalten von Druckern und Ports
Datei- & Druckinfrastruktur	Gruppenrichtlinien (GPO)	Automatisches Erstellen von Druckern in definierten GPOs
Kommunikation & Collaboration	Microsoft Exchange & Office 365	Verwaltung von Nutzern, Postfächern, Verteilerlisten und Berechtigungen
Kommunikation & Collaboration	Microsoft Teams	Erstellen und Verwalten von Nutzern sowie Gruppen und Bereichen
Kommunikation & Collaboration	Cisco Callmanager	Erstellen und Verwalten von Telefonen, Softphones, Weiterleitungen und Voicemail

Kategorie	Systeme	Funktionsumfang
Kommunikation & Collaboration	WebEx	Erstellen und Verwalten von Nutzern sowie Gruppen und Bereichen
Endpoint & Geräteverwaltung	Microsoft Intune	Hinzufügen und einfaches Verwalten von mobilen Geräten
Endpoint & Geräteverwaltung	Baramundi	Erstellen und Löschen von Geräten in logischen Gruppen; Zuweisen von Jobs
Speichersysteme	PowerScale	Auslesen von Speicherquoten
Servicemanagement	TOPdesk	API-Zugriff; Anlegen und Auslesen von Assets; Erstellen und Bearbeiten von Changes und Changeaktivitäten; Ablegen von Dokumenten in den Stammdaten

1.4 Projektrahmen

Parameter	Wert
Auftraggeber	Staatsbibliothek zu Berlin
Anzahl verwalteter Identitäten	Insgesamt 4.300 Konten davon ca. 2.500 Mitarbeiterkonten
Geplanter Projektzeitraum	6 – 12 Monate
Projektbeginn (geplant)	01.08.2026

2 Gegenstand der Leistung

2.1 Überblick

Gegenstand der Ausschreibung ist die Ablösung der bestehenden IAM-Lösung (Tools4ever) sowie die Einführung einer modernen, On-Premise betriebenen Identity- und Access-Management-Plattform für die Staatsbibliothek zu Berlin. Die neue Lösung soll ca. 3.500 Benutzeridentitäten verwalten und vollständig in die bestehende IT-Systemlandschaft integriert werden.

Der Auftragnehmer erbringt folgende Leistungen:

- Lizenzierung der IAM-Plattformsoftware
- Implementierung, Konfiguration und Integration in alle relevanten Zielsysteme
- Migration der Bestandsdaten aus dem bestehenden Tools4ever-System
- Schulung der Administratoren und First-Level-Support

2.2 Funktionale Anforderungen

Hinweis: Dieser Abschnitt beschreibt die geforderten Funktionen aus Sicht des Auftraggebers.

2.2.1 Benutzermanagement

Funktion	Beschreibung
Benutzer erstellen	Vorlagen für Rollen und Abteilungen; Auswahllisten für Standorte, Adressen, Einrichtungen, Abteilungen und Rollen; automatische Vergabe von Accountnamen; E-Mail-Einrichtung; Erstellen von Telefonnummern und Softphones; Standard-Berechtigungen, Verteiler und Postfachzugriffe

Funktion	Beschreibung
Benutzer bearbeiten	Änderung aller relevanten Informationen: Einrichtung, Abteilung, Namen, Adressen, Büro, E-Mail-Adresse, Laufzeit
Benutzer in Einrichtung verschieben	Ändern der Vorlage, Änderung aller relevanten AD-Attribute, Verschieben des Nutzers, Migration von Profil- und Home-Verzeichnissen beim Einrichtungswechsel
Benutzer deaktivieren und löschen	Deaktivierung und Verschiebung im AD, Löschen des Nutzers und aller persönlichen Verzeichnisse und Mailboxen, Hinweise auf Managergruppen
Benutzer wiederherstellen	Aktivierung und Rückverschiebung in die ursprüngliche OU, Wiederherstellung aus dem AD-Papierkorb, Auflisten von Home- und Profilpfaden
Umbenennen von Benutzern	Änderung aller relevanten Informationen bei Namensänderung (Vorname, Nachname, Titel, E-Mail-Adresse)
Passwörter zurücksetzen	Rücksetzung mit Passwortgenerierung, Erstellen von Passwortbriefen (Vorlage), optionale PIN-Absicherung
Rollenmanagement	Vorgesetzter, Mitarbeiter, Praktikant, Externer
Zusatz-Accounts verwalten	Personalrat, Admin-Konten; optional: Verknüpfung/Verweis auf Mitarbeiter-Account in anderen Domänen
Dienst- und Sonderkonten	Erstellen und Verwalten von Dienstkonten, Sonderkonten für gemeinsame Nutzung (z. B. Wachen), Service-Accounts, Dienstleister- und externe Accounts
Migrieren von Benutzern	Überführen alter Accounts in neue Strukturen
Gruppenmanagement	Hinzufügen, Entfernen, Kopieren von Nutzern; definierte Gruppenauswahl
Benutzervorlagen	Vorlagen für Rollen und Abteilungen

2.2.2 E-Mail- und Exchange-Management

Funktion	Beschreibung
Postfächer verwalten	Erstellen, Verschieben und Kontingente setzen
E-Mail-Adressen ändern	Hinzufügen, Entfernen und Verwalten von E-Mail-Adressen
Verteiler verwalten	Erstellen, Bearbeiten, Löschen; Mitglieder hinzufügen/entfernen; Gruppen verschachteln oder auflösen; dynamische Verteiler mit automatischer Befüllung nach Kriterien (Hintergrund-Job)
Verteiler-Manager	Berechtigung zur Mitgliederverwaltung für mehrere Nutzer
Funktionspostfächer	Anlegen von freigegebenen Postfächern, Ressourcen- und Raumpostfächern; Einrichtung automatischer Raumbuchung
Postfachzugriffsrechte	Verwalten von Berechtigungen (Vollzugriff, Senden als, Senden im Auftrag, Kalenderfreigabe) über Benutzer und Gruppen
Abwesenheitsnotizen	Verwaltung auf alle Postfachtypen
Kalenderberechtigungen	Einrichten und Verwalten von Kalenderfreigaben
Funktionspostfach-Manager	Hinterlegen von Personen und Gruppen als Postfachverwalter

2.2.3 Verzeichnis- und Berechtigungsmanagement (File Server)

Funktion	Beschreibung
Rechte auf Ordnern einrichten	Anlegen von Zugriffsgruppen und Schreiben ins Dateisystem; Schreib-, Lese- und Auflistungsrechte
Manager / Untermanager hinterlegen	Hinterlegen und Verwalten von Nutzern und Gruppen als Verantwortliche für Berechtigungen
Rechte für Benutzer und Gruppen verwalten	Verwaltung über die Oberfläche
Berechtigungen migrieren	Automatische Migration und Anpassung bestehender Berechtigungen in neue Strukturen
Genehmigungsworkflows	Benachrichtigung und Freigabe durch zuständige Manager
Berechtigungsreport	Für Administratoren und Nutzer

2.2.4 Telefonmanagement (Cisco Callmanager)

Funktion	Beschreibung
Softphones anlegen	Erstellen mit automatischer Nummernvergabe
Telefone einrichten	Als Anmelde- und Funktionstelefon
Zurücksetzen	Zurücksetzen auf Werkseinstellungen oder Standard-Konfiguration
Rufgruppen einrichten	Anlegen und Verwalten von Rufgruppen
Weiterleitungen einrichten	Einrichtung von Anrufweiterleitungen (Dienstgeräte)
Bereinigung	Entfernen aller Einstellungen zu Nummer oder Gerät aus dem Callmanager
Voicemail verwalten	Einrichten, Löschen, PIN zurücksetzen
AD-Synchronisation	Manuelles Starten der Synchronisation mit Active Directory

2.2.5 Druckermanagement

Funktion	Beschreibung
Drucker anlegen	Namenskonvention vorgeben; Drucker auf verschiedenen Druckservern anlegen; Auswahl an Treibern; Erstellen von Zugriffsgruppen
GPO-Anpassung	Automatisches Erstellen von Druckern in definierten Gruppenrichtlinien
Zugriff verwalten	Nutzern, Gruppen und Geräten Zugriff gewähren und entziehen
Drucker löschen	Löschen auf dem Druckserver, Ports und Verwaltungsgruppen
Drucker umbenennen	Drucker, Port und Verwaltungsgruppen
Treiberverwaltung	Treiber für einzelne Drucker oder Modellreihen wechseln
Drucker konfigurieren	Anpassung von Druckerkonfigurationen

2.2.6 Reporting

Report	Inhalt
Benutzer-Report	Auflistung von Zugriffen (Verzeichnisse, Postfächer, Drucker) aus Gruppenmitgliedschaft; Anmeldedaten (letzte Anmeldung, Ablaufdatum); OU-Zugehörigkeit
Verzeichnis-Report	Nutzer nach Zugriffstyp (Lesen, Schreiben, Manager); Auflösung von Gruppenmitgliedschaften (effektiver Zugriff); Vererbungsinformationen
Telefon-Report	Aktivierte Features je Nummer/Nutzer (z. B. Auslandstelefonie); angemeldete Telefone; Weiterleitungen; Fehlkonfigurationen
Exchange-Report	Füllgrad der Datenbanken; Postfachgrößen; Zugriffsrechte auf Postfächern und Kalendern
Gruppen-Report	Auflösung von Gruppenmitgliedschaften

2.2.7 Self-Service-Portal

Für Nicht-IT-Mitarbeiter
<ul style="list-style-type: none"> • Anpassen eigener Daten (Raum, Standort, Adresse per Auswahlliste, Mobilnummer, individuelle Felder) • Persönliche PIN für Passwort-Rücksetzung festlegen • Anzeige von Home- und Postfach-Auslastung • Einrichten von E-Mail-Weiterleitungen • Links zu relevanten Systemen (TOPdesk, Callmanager)
Für IT-Beauftragte
<ul style="list-style-type: none"> • Auflisten von Verzeichnis-, Postfach- und Drucker-Berechtigungen (gefiltert nach Abteilung/Manager) • Auflisten von Vorgesetzten und Mitarbeitern nach Abteilung • Raumanpassungen nach Abteilung • Passwort-Rücksetzung mit Nutzer-PIN • Links zu relevanten Systemen (TOPdesk, Callmanager)

2.3 Abgrenzung – Nicht Gegenstand der Leistung

Folgende Leistungen sind ausdrücklich nicht Bestandteil der Leistung:

- Beschaffung und Bereitstellung von Server-Hardware
- Anpassung oder Restrukturierung von Quellsystemen (z. B. AD-Umstrukturierung)
- Betrieb und Hosting der IAM-Lösung nach Go-Live (verbleibt beim Auftraggeber)

3 Anforderungen an den Auftragnehmer

3.1 Personalanforderungen

Der Auftragnehmer hat für die Projektlaufzeit und darüber hinaus mindestens folgende Rollen namentlich zu benennen und deren Qualifikation nachzuweisen:

Rolle	Aufgaben und Anforderungen
IAM-Architekt / Technischer Berater	Verantwortlich für Systemarchitektur, Integrationskonzept und technische Gesamtsteuerung; nachgewiesene Erfahrung mit vergleichbaren IAM-Implementierungen
Support-Ansprechpartner (nach Go-Live)	Benannter, persönlicher Ansprechpartner für den Auftraggeber nach Projektabschluss; erreichbar innerhalb definierter Reaktionszeiten (siehe Abschnitt 6)

3.2 Projektdurchführung

Die Projektdurchführung erfolgt hybrid – eine Kombination aus Vor-Ort-Präsenz beim Auftraggeber und Remote-Arbeit. Der Auftragnehmer hat dabei folgendes sicherzustellen:

- Schlüsselphasen (Kick-off, Konzeptabnahme, Testabnahme, Go-Live) finden vor Ort beim Auftraggeber statt
- Remote-Zugriffe auf Systeme des Auftraggebers erfolgen ausschließlich über freigegebene, gesicherte Zugangswege (z. B. VPN)
- Termine und Präsenzpfllichten werden im Projektplan verbindlich vereinbart

3.3 Compliance- und Sicherheitsanforderungen

Der Auftragnehmer ist verpflichtet, folgende Anforderungen vollumfänglich einzuhalten und auf Verlangen nachzuweisen:

Anforderung	Beschreibung
BSI IT-Grundschutz	Die IAM-Lösung sowie alle projektbezogenen Tätigkeiten müssen den Anforderungen des BSI IT-Grundschutzes entsprechen. Relevante Bausteine (insbesondere ORP.4 – Identitäts- und Berechtigungsmanagement) sind zu berücksichtigen. Auf Anforderung ist eine Dokumentation der umgesetzten Maßnahmen vorzulegen.
DSGVO / Datenschutz	Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen eines abzuschließenden Auftragsvertrags (AVV). Alle Mitarbeitenden mit Datenzugang sind auf Datenschutzvorschriften zu verpflichten. Personenbezogene Daten verbleiben ausschließlich auf Systemen innerhalb der Bundesrepublik Deutschland bzw. des EWR.

3.4 Dokumentation

Sämtliche Projektdokumentation, technische Unterlagen, Handbücher, Schulungsunterlagen sowie die gesamte Projektkommunikation sind zwingend in deutscher Sprache zu erbringen. Dies gilt auch für Benutzeroberflächen der gelieferten Lösung.

3.5 Support, Wartung und Pflege

Für alle Module des gelieferten Systems ist ein umfassender Software-Support zu leisten, der auch Hauptreleases umfasst. Die AG kann stets die aktuelle Version der Software einsetzen.

Bei Software- und Systemfehlern steht der Anbieter im Rahmen des Software-Wartungsvertrages gem. Preisblatt Pos. 1.1 bis 1.3 zur Problemlösung zur Verfügung. Ein Remotezugang zu den Servern des Systems wird eingerichtet. Das Software-Gesamtsystem der Wartung umfasst alle gelieferten Module, auch von Drittherstellern sowie alle mitgelieferten Installationspakete.

Der Support erfolgt in deutscher Sprache und wird durch den AN gewährleistet.

Reise- und Nebenkosten für vor-Ort Arbeiten sind im Pauschalpreis inbegriffen.

Der AN muss ein System zur programmgesteuerten Verwaltung von Änderungsanfragen (Change Requests) bzw. den zugehörigen Änderungsmaßnahmen implementieren (Ticket-System). Der AN muss für die Umsetzung von Änderungsanfragen (Change Requests) eine Aufwandsabschätzung (inklusive Zeitplanung) erstellen und eine Abschätzung der Bearbeitungszeit abgeben.

3.6 Exit Management

Zum Ende der Vertragslaufzeit muss der AN die AG unterstützen, eine reibungslose Übergabe der ITSM-Software sowie den Betrieb der ITSM-Software an einen nachfolgenden Dienstleister zu gewährleisten.

Der AN ist verpflichtet, mit dem nachfolgenden Dienstleister für einen geregelten Übergang aktiv zusammenzuarbeiten. Eine reibungslose Übertragung der Verantwortung muss vom AN gewährleistet werden.

Die Parteien vereinbaren eine dem Leistungsgegenstand angemessene Übergangszeit von drei Monaten für die Übernahme der Leistungen durch die AG oder einen Dritten.

Der AN unterstützt die AG bei der Erstellung von Plänen, welche Leistungen in welchem Umfang und zu welchem Zeitpunkt an die AG oder einen Dritten übergehen.

Der AN stellt der AG sämtliche Unterlagen, die die AG oder ein Dritter zur Übernahme der Leistung benötigt, zur Verfügung. Der AN unterstützt die AG oder den Dritten aktiv bei der Übergabe der Leistungen.

3.7 Ergänzende Dienstleistungen

Ergänzend der Erstimplementierung müssen vom AN ergänzende Dienstleistungen bei der Konfiguration der IAM-Software nach den konkreten Anforderungen der AG erbracht werden. Die ergänzenden Dienstleistungen dienen der Feinkonfiguration, der Implementierung des Datenaustausches über die Schnittstellen, der Einrichtung von Strukturen, Berichten und Berechtigungen sowie weitergehenden Anforderungen auf Grundlage der Softwarelösung. Es wird davon ausgegangen, dass die erforderliche Unterstützungsleistung einen Aufwand von 10 Personentagen je 8 Stunden pro Jahr nicht überschreitet.

4 Liefergegenstände und Ergebnisse

4.1 Zu liefernde Dokumente

Der Auftragnehmer hat folgende Dokumente in deutscher Sprache zu erstellen und dem Auftraggeber zu übergeben:

Dokument	Inhalt
Technisches Konzept / Architekturdokumentation	Beschreibung der Systemarchitektur, Integrationskonzept für alle Zielsysteme, Datenflussdokumentation, Sicherheitskonzept
Installationsdokumentation	Vollständige Dokumentation der Installation und Konfiguration der IAM-Plattform; reproduzierbar und nachvollziehbar für den Auftraggeber
Betriebshandbuch für Administratoren	Anleitungen für den laufenden Betrieb, Wartung, Fehlerbehebung und Konfigurationsänderungen durch das IT-Personal des Auftraggebers

Alle Dokumente sind im Format Microsoft Word (.docx) oder PDF zu liefern und müssen den Anforderungen des BSI IT-Grundschutzes entsprechen.

4.2 Technische Liefergegenstände

Folgende technische Ergebnisse sind vom Auftragnehmer bereitzustellen und zur Abnahme vorzulegen:

Liefergegenstand	Abnahmekriterium
Vollständig installiertes und konfiguriertes IAM-System	Alle Kernfunktionen gemäß Abschnitt 2.2 sind lauffähig und getestet
Alle Integrationen in Betrieb	Sämtliche Zielsysteme (AD, Exchange, Cisco, Azure AD, Teams, Intune, WebEx, TOPdesk, Baramundi, PowerScale) sind vollständig angebunden und funktionsfähig
Migrierte Bestandsdaten aus Tools4ever	Alle relevanten Bestandsdaten (Benutzer, Gruppen, Berechtigungen, Vorlagen) sind vollständig und korrekt überführt; Abweichungen sind dokumentiert

4.3 Abnahme

Die Abnahme der Liefergegenstände erfolgt dreistufig:

Stufe	Abnahmeform	Beschreibung
1	Stufenweise Abnahme je Integrationspaket	Jede Systemintegration wird nach Fertigstellung separat abgenommen. Der Auftragnehmer legt ein Testprotokoll vor. Die Abnahme gilt als erteilt, wenn alle definierten Testfälle erfolgreich durchlaufen wurden.
2	Abnahme durch Fachbereich + IT gemeinsam	Nach Abschluss aller Integrationspakete erfolgt eine Gesamtabnahme unter Beteiligung von IT-Bereich und fachlich betroffenen Organisationseinheiten. Kernprozesse werden praxisnah geprüft.
3	Formale Abnahme durch IT-Leitung	Nach erfolgreicher Abnahme durch Fachbereich und IT erteilt die IT-Leitung die formale Gesamtabnahme schriftlich. Erst damit gilt das Projekt als vollständig abgeschlossen.

5 Zeitplan und Meilensteine

5.1 Projektbeginn

Das Projekt beginnt schnellstmöglich nach Zuschlagserteilung. Der genaue Starttermin wird im Rahmen des Kick-off-Meetings verbindlich festgelegt.

5.2 Projektphasen und Meilensteine

Der Auftragnehmer legt einen detaillierten Projektplan vor, der alle unten genannten Phasen und Meilensteine abbildet. Der Plan bedarf der schriftlichen Genehmigung durch den Auftraggeber vor Projektbeginn. Abweichungen vom genehmigten Zeitplan sind unverzüglich zu melden und gemeinsam abzustimmen.

#	Phase	Inhalte	Dauer	Meilenstein
1	Kick-off und Projektplanung	Abstimmung Projektziele, Rollen und Verantwortlichkeiten; Finalisierung und Genehmigung des Projektplans; Einrichtung der Projektkommunikation	1 – 2 Wo.	Genehmigter Projektplan
2	Ist-Analyse und Konzeptphase	Aufnahme der bestehenden Tools4ever-Umgebung; Erstellung Architektur- und Integrationskonzept; Abstimmung mit Auftraggeber	3 – 4 Wo.	Abgenommenes Fachkonzept
3	Implementierung und Konfiguration	Installation der IAM-Plattform (On-Premise); Grundkonfiguration, Rollenmodell, Vorlagen und Workflows	4 – 6 Wo.	Lauffähiges Basissystem
4	Integration der Zielsysteme	Schrittweise Anbindung aller Zielsysteme; stufenweise Abnahme je Paket	6 – 8 Wo.	Alle Integrationen abgenommen
5	Migration der Bestandsdaten	Überführung aller relevanten Daten aus Tools4ever; Validierung und Dokumentation	2 – 3 Wo.	Migrationsprotokoll abgenommen
6	Testphase / Pilotbetrieb	Durchführung definierter Testfälle; Pilotbetrieb mit ausgewählten Nutzern; Fehlerbehebung	3 – 4 Wo.	Abnahme Testprotokoll
7	Schulung der Administratoren und Anwender	Durchführung der Schulung (Remote); Übergabe der Schulungsunterlagen	1 – 2 Wo.	Schulung abgenommen
8	Go-Live und Produktivbetrieb	Übergang in den Produktivbetrieb; Hypercare-Phase; formale Gesamtabnahme durch IT-Leitung	2 Wo.	Formale Gesamtabnahme

Gesamtprojektlaufzeit (indikativ): 6 – 12 Monate ab Projektstart

5.3 Berichtswesen

Der Auftragnehmer ist verpflichtet, dem Auftraggeber regelmäßig über den Projektfortschritt zu berichten:

- Wöchentlicher Statusbericht (schriftlich, per E-Mail) mit Fortschritt, offenen Punkten und Risiken
- Monatliches Jour fixe (vor Ort oder remote) zur gemeinsamen Steuerung
- Sofortige Meldung bei drohenden Terminverzügen oder kritischen Problemen

6 Anforderungskatalog

Der nachfolgende Anforderungskatalog listet alle funktionalen und nicht-funktionalen Anforderungen an die IAM-Lösung.

Die folgenden Features sind Muss-Anforderungen (Ausschlusskriterien). Sie müssen zwingend von der Software unterstützt werden. Ein Nichtvorhandensein führt zum Ausschluss des Angebotes.

6.1 Active Directory Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss in der Lage sein, Benutzer in Active Directory anzulegen, zu bearbeiten, zu sperren/entsperren und zu löschen.
2	Es muss konfigurierbar sein, dass im Anlageprozess im Active Directory die Benutzer auf Basis der Abteilung, Niederlassung oder des Benutzertyps automatisch in der richtigen OU angelegt werden.
3	Das Initialpasswort für den Benutzer muss automatisch generiert werden können (die Passwortrichtlinie muss dabei berücksichtigt werden). Es müssen flexible Möglichkeiten bestehen, wie der Benutzer sein Initialpasswort erfährt.

6.2 Audit und Dokumentation Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss jede Änderung lückenlos dokumentieren. Mindestens vorgesehen werden muss: Antragsteller und Zeitpunkt, alle Genehmiger und Zeitpunkt der Genehmigung, alle Änderungen, die in Zielsystemen durchgeführt wurden.

6.3 Berechtigungen Muss-Anforderungen

Nr.	Anforderung
1	Bei der Anlage und Bearbeitung von Mitarbeitern muss es möglich sein, Berechtigungen bis auf Feldebene zumindest für die Aktionen 'Anzeige' und 'Bearbeitung' zu vergeben.
2	Die Software muss ein internes Berechtigungssystem haben. Dieses muss rollenbasiert sein. Es muss möglich sein, Berechtigungen auf Basis von Standort und Abteilung zu vergeben. Für Mitarbeiterdaten müssen die Berechtigungen bis auf Feldebene einstellbar sein. Es müssen dabei zumindest die Funktionen 'Anzeigen' und 'Bearbeiten' einstellbar sein.

6.4 Fileserver Muss-Anforderungen

Nr.	Anforderung
1	Bei den erzeugten Fileserver-Gruppen müssen Namenskonvention, Gruppentyp sowie der Speicherort (OU im AD) konfigurierbar sein. Es müssen zumindest die Systeme AGDLP, AGP/AGGP und AUP/AUUP unterstützt werden.
2	Für Multidomain-Umgebungen muss das Konzept AGDLP mit lokaler Gruppe in der Domain des Fileservers und globaler Gruppe in der Domain des Benutzers unterstützt und automatisch umgesetzt werden können.
3	Beim Report für ein Verzeichnis muss es die Möglichkeit geben, Unterverzeichnisse miteinzubeziehen, aber gleichzeitig nur die Differenzen der (effektiven) Berechtigungen anzuzeigen.
4	Das System muss die Möglichkeit bieten, Berechtigungen auf Fileservern zu ändern. Dabei dürfen nur Microsoft Best Practices zum Einsatz kommen. Die notwendigen Gruppen muss die Software selbst erzeugen, aktualisieren und löschen. Die Namenskonvention für die automatisch erzeugten Gruppen muss konfigurierbar sein.
5	Die Software muss die einfache Analyse von Verzeichnisberechtigungen unterstützen. Die Informationen müssen grafisch aufbereitet sein. Per Mausklick müssen die effektiven Berechtigungen eines Benutzers angezeigt werden können. Der Berechtigungspfad jedes berechtigten Benutzers muss ersichtlich sein.
6	Die Software muss die Möglichkeit bieten, neue Verzeichnisse anzulegen und bestehende Verzeichnisse zu löschen. Darüber hinaus muss es die Möglichkeit geben, Verzeichnisse umzubenennen (dieser Vorgang muss ggf. auch alle involvierten Gruppen umbenennen).
7	Es müssen alle Arten von Fileservern angebunden werden können, die CIFS und/oder SMB unterstützen. Insbesondere müssen Appliances von NetApp und EMC unterstützt werden.
8	Für Verzeichnisberechtigungen muss es Reporting-Möglichkeiten in PDF und Excel geben.
9	Bei der Definition von Dateneigentümern von Fileserver-Verzeichnissen ist eine granulare Gestaltung der möglichen Aktionen des Dateneigentümers erforderlich. Mindestens erforderlich sind: Berechtigungen

Nr.	Anforderung
	anzeigen, Berichte ausführen, Berechtigungen ändern, Unterverzeichnisse anlegen/umbenennen/löschen, Vererbung verändern.
10	Bei der Anzeige der Fileserver-Berechtigungen muss von der obersten Ebene ausgehend die Anzahl der kumulierten, abweichenden Berechtigungen in Unterverzeichnissen sichtbar sein, damit von oberster Ebene abwärts identifizierbar ist, in welchen Verzeichnissen sich Berechtigungen ändern bzw. neue Berechtigungen hinzukommen.

6.5 Microsoft Exchange Muss-Anforderungen

Nr.	Anforderung
1	Bei den erzeugten Exchange-Gruppen müssen Namenskonvention, Gruppentyp sowie der Speicherort (OU im AD) konfigurierbar sein.
2	Das System muss die Möglichkeit bieten, Berechtigungen auf Postfächern und Ordnern in Microsoft Exchange zu ändern. Dabei dürfen nur Microsoft Best Practices zum Einsatz kommen. Die notwendigen Gruppen muss die Software selbst erzeugen, aktualisieren und löschen. Die Namenskonvention für die automatisch erzeugten Gruppen muss konfigurierbar sein.
3	Die Software muss die einfache Analyse von Postfach- und Ordnerberechtigungen in Microsoft Exchange unterstützen. Die Informationen müssen grafisch aufbereitet sein. Per Mausklick müssen die effektiven Berechtigungen eines Benutzers angezeigt werden können. Der Berechtigungspfad jedes berechtigten Benutzers muss ersichtlich sein.
4	Es müssen hybride Exchange-Umgebungen in Verbindung mit Microsoft Exchange Online gleichermaßen unterstützt werden.
5	Exchange-Postfächer müssen automatisch angelegt werden können. Die E-Mail-Adresse muss entweder per Scripting oder per Empfängerrichtlinie erstellbar sein. Die Postfachdatenbank muss automatisch auf Basis des Standorts des Benutzers ausgewählt werden können. Die Auswahllogik muss darüber hinaus 'kleinste Datenbank' und 'Datenbank mit wenigsten Postfächern' unterstützen.
6	Die Beantragung von Zugriff auf freigegebene Postfächer und öffentliche Ordner muss über die Self-Service-Oberfläche möglich sein. Es muss gesteuert werden können, welche Postfächer zur Beantragung zur Verfügung stehen und welche nicht.
7	Automatisch angelegte Gruppen für Exchange-Berechtigungen müssen konfigurierbar aus dem Exchange-Adressbuch ausgeblendet werden können oder auch nicht.
8	Die Software muss es ermöglichen, dass der Vorgesetzte eines Mitarbeiters dessen Abwesenheitsnotiz setzen kann. Die möglichen Texte müssen auf organisationsweit einstellbaren Templates basieren können.

6.6 Microsoft 365 und Azure AD Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss eine Integration mit den Diensten von Microsoft 365 bieten.
2	Die Software muss in Azure Active Directory integrierbar sein. Dabei müssen sowohl hybride (synchronisierte, lokale Active Directory Benutzer) als auch native Onlinebenutzer unterstützt werden. Darüber hinaus müssen alle Arten von M365-Gruppen unterstützt werden, einschließlich verschachtelter Gruppen.
3	Das System muss die Möglichkeit bieten, Berechtigungen auf Postfächern und Ordnern in Microsoft Exchange Online zu ändern. Dabei dürfen nur Microsoft Best Practices zum Einsatz kommen. Die notwendigen Gruppen muss die Software selbst erzeugen und aktualisieren. Die Namenskonvention für die automatisch erzeugten Gruppen muss konfigurierbar sein.
4	Die Software muss die einfache Analyse von Postfach- und Ordnerberechtigungen in Microsoft Exchange Online unterstützen. Die Informationen müssen grafisch aufbereitet sein. Per Mausklick müssen die effektiven Berechtigungen eines Benutzers angezeigt werden können.
5	Exchange-Online-Postfächer müssen automatisch angelegt werden können. Die E-Mail-Adresse muss entweder per Generierungsregel oder per Empfängerrichtlinie erstellbar sein.

Nr.	Anforderung
6	In M365 muss die Zuweisung von Lizenzen und Apps möglich sein. Darüber hinaus muss angezeigt werden können, welche Benutzer über welche Lizenzen und Apps verfügen. Dabei müssen sowohl direkte Zuordnungen als auch Zuordnungen über Gruppen unterstützt werden.
7	Es muss die Möglichkeit geben, anzuzeigen, ob Gastbenutzer existieren, denen eine Lizenz zugeordnet ist.
8	Es muss die Möglichkeit geben, anzuzeigen, ob Gastbenutzer existieren, die Mitglied eines Teams in Microsoft Teams sind.

6.7 OneDrive Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss anzeigen können, welche Dateien und Ordner in OneDrive über Sharing Links geteilt werden und ob diese Links mit Passwort abgesichert sind.

6.8 Microsoft SharePoint Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss die einfache Analyse von Berechtigungen in Microsoft SharePoint unterstützen. Die Informationen müssen grafisch aufbereitet sein. Per Mausklick müssen die effektiven Berechtigungen eines Benutzers angezeigt werden können. Der Berechtigungspfad jedes berechtigten Benutzers muss ersichtlich sein.
2	Es müssen SharePoint Online von der Software gleichermaßen unterstützt werden.
3	In der Software muss es möglich sein, Berechtigungen in Microsoft SharePoint Online zu setzen.
4	Beim Setzen von Berechtigungen in SharePoint Online muss die Lösung sowohl bestehende Standardgruppen verwenden können als auch bei Bedarf automatisch neue SharePoint-Gruppen nach einer konfigurierbaren Namenskonvention erzeugen können.

6.9 Passwort-Reset Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss über ein Portal zum Zurücksetzen von Kennwörtern verfügen. Es müssen dabei zumindest Active Directory Kennwörter zurücksetzbar sein.
2	Zur Authentifizierung muss das Portal dem Benutzer die Beantwortung einer konfigurierbaren Anzahl an Geheimfragen ermöglichen.

6.10 PowerShell Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss die Möglichkeit haben, eigene PowerShell-Skripte durchzuführen.

6.11 Self Service Muss-Anforderungen

Nr.	Anforderung
1	Aus Gründen der Vereinfachung darf es keine Trennung zwischen Administrationsoberfläche und Self-Service-Oberfläche geben. Die Steuerung darf nur auf Basis von Berechtigungen erfolgen. Es darf keine Installation zusätzlicher Tools für Self Service oder Adminoberfläche notwendig sein.
2	Die Software muss eine für den Benutzer verständliche Self-Service-Oberfläche bieten. Diese muss zumindest folgende Funktionen bieten: Anfragen von Ressourcen und Berechtigungen sowie eigenständige Änderung von speziell freigeschalteten Benutzerattributen.

Nr.	Anforderung
3	Die Verfügbarkeit der Ressourcen im Self Service muss eingeschränkt werden können. Es sollen dem Benutzer nur die Ressourcen angezeigt werden, die für seine Abteilung, seinen Standort oder seine Firma freigegeben sind.

6.12 Support und Dokumentation Muss-Anforderungen

Nr.	Anforderung
1	Der Support muss deutschsprachig sein.
2	Der Support muss werktags zwischen 9:00 und 16:00 Uhr erreichbar sein.
3	Die Dokumentation muss zu 100% in deutscher Sprache vorliegen.

6.13 Systemumgebung Muss-Anforderungen

Nr.	Anforderung
1	Als Datenbanksystem muss zwingend Microsoft SQL Server zum Einsatz kommen.
2	Der Betrieb des Anwendungsservers muss auf dem Betriebssystem Windows Server 2022/2025 möglich sein.
3	Die Benutzeroberfläche muss zu 100% in deutscher Sprache verfügbar sein.
4	Die Software muss zu 100% webbasiert sein. Es dürfen keine Clients zum Einsatz kommen, die auf einem PC installiert werden müssen.
5	Für die Anmeldung an der Weboberfläche muss eine Integration mit Active Directory über Kerberos gegeben sein. Der Anwender darf sein Passwort nicht erneut eingeben müssen (SSO).

6.14 Third-Party-Integrationen Muss-Anforderungen

Nr.	Anforderung
1	Die individuellen Scripts müssen zwingend an bestimmte Systemereignisse geknüpft werden können. Der Zugriff auf interne Systemstrukturen muss gewährleistet sein, damit systemtechnische Abläufe tatsächlich beeinflusst werden können.

6.15 User Lifecycle und Profile Muss-Anforderungen

Nr.	Anforderung
1	Die Software muss die Abbildung des Lifecycles der Mitarbeiter unterstützen. Eintritte, Änderungen und Austritte müssen über einfach zu bedienende Formulare möglich sein. An keinem Punkt dürfen Kenntnisse in Active Directory, Exchange oder anderen IT-Produkten notwendig sein.
2	Die Software muss Ressourcen und Berechtigungen automatisch auf Basis von Attributen (Abteilung, Standort sowie jegliche weiteren Attribute) des Mitarbeiters zuordnen können. Es muss auch bei Änderungen eine entsprechende Prüfung erfolgen, sodass nicht mehr zutreffende Berechtigungen automatisch entfernt werden.
3	Es muss eine Funktion zur Verfügung gestellt werden, die über sogenanntes 'Role Mining' die Anlage von Geschäftsrollen vereinfacht bzw. ermöglicht.
4	Es muss eine Funktion zur Verfügung gestellt werden, über die sich Rollen an Benutzer und Benutzer an Rollen angleichen lassen.
5	Es müssen Auswertungsfunktionen zur Verfügung gestellt werden, mit denen Individualberechtigungen eines Mitarbeiters (im Vergleich zu seinen Rollen) dargestellt werden können. Diese Auswertung muss auch auf Abteilungsbasis zur Verfügung gestellt werden.
6	Die Software muss die Möglichkeit bieten, die unterschiedlichen Zustände/Phasen eines Mitarbeiters (z. B. Aktiv, Elternzeit, Ausgetreten) abzubilden. Jede Phase muss einfach mit bestimmten Aktionen ausgestattet werden können, ohne Programmierkenntnisse oder Anpassungen in Konfigurationsdateien.

Nr.	Anforderung
7	Die Funktionen für die Zustände/Phasen müssen vorrangig vor den automatisch zugeordneten Berechtigungen via Rollen/Profilen gelten.

6.16 Workflows Muss-Anforderungen

Nr.	Anforderung
1	Bei der Beantragung mehrerer Anwendungsberechtigungen für einen Benutzer muss es im Genehmigungsworkflow die Möglichkeit geben, dass jeder Genehmiger nur die Berechtigungen genehmigt, für die er zuständig ist. Es sind separate Kommentarfelder vorzusehen.
2	Zusätzlich zu den Standardfeldern muss es die Möglichkeit geben, benutzerdefinierte Felder zu konfigurieren. Es sind zumindest Textboxen, Auswahlboxen und Checkboxen vorzusehen. Die Erforderlichkeit der Eingabe muss einstellbar sein und für Administratoren überschreibbar.

6.17 Rezertifizierung Muss-Anforderungen

Nr.	Anforderung
1	Von der Rezertifizierung müssen Active Directory Gruppen und Ordner auf dem Fileserver berücksichtigt werden.
2	Es muss die Möglichkeit geben, alle Berechtigungen eines Benutzers bzw. alle Berechtigungen auf einer Ressource mit einem Klick pauschal zu rezertifizieren.
3	Es muss die Möglichkeit geben, zu konfigurieren, ob Unterverzeichnisse bei der Rezertifizierung berücksichtigt werden sollen oder nicht.
4	Von der Rezertifizierung müssen Anwendungen, Anwendungsberechtigungen (Rollen) und sonstige Ressourcen ebenfalls berücksichtigt werden.
5	Die Ergebnisse der Rezertifizierung müssen von einem Auditor mit speziellen Berechtigungen im Read-Only-Modus online kontrolliert werden können.

6.18 Technische Umgebung und Hosting Muss-Anforderungen

Nr.	Anforderung
1	Das System muss als On-Premise-Lösung verfügbar sein und über eine Virtual Appliance oder Native Installation auf den eigenen Servern des Auftraggebers gehostet werden können.
2	Das System muss unter VMware vSphere ESXi ab Version 8 lauffähig sein.
3	Es müssen SQL-Datenbanken unterstützt werden; MS SQL Server ab Version 2019 ist zwingend erforderlich.
4	Das System muss DSGVO-konform betrieben werden können.

6.19 Schnittstellen (Basisfunktionen) Muss-Anforderungen

Nr.	Anforderung
1	Eine Anbindung an Active Directory (On-Premises) muss möglich sein.
2	Eine Anbindung an Azure Active Directory muss möglich sein.
3	Das Hinzufügen individueller Informationen und Anlagen (Dokumente, Dateien) zu Objekten muss möglich sein.
4	Zugriff auf Microsoft Exchange Online und Microsoft Exchange On-Premises muss unterstützt werden.
5	Zugriff auf File- und Druckerserver muss möglich sein.
6	Der Import von Daten per SQL und CSV muss automatisiert möglich sein.
7	Der API-Zugriff muss vollständig dokumentiert und nutzbar sein.

Nr.	Anforderung
8	Eine Telefonie-Anbindung (Cisco Callmanager) muss unterstützt werden.
9	Eine Anbindung an Microsoft 365 muss möglich sein.
10	Die Nutzung von eigenen PowerShell-Skripten muss möglich sein.

6.20 Anpassbarkeit (No-Code-Plattform) Muss-Anforderungen

Nr.	Anforderung
1	Anpassungen und Einstellungen innerhalb des Standards dürfen an keiner Stelle im System Programmierkenntnisse erfordern (No-Code-Plattform).
2	Zusätzliche Registerkarten, Felder und Datenbankfelder müssen frei definierbar sein.
3	Individuelle Feldnamen müssen festlegbar und Pflichtfelder müssen anpassbar sein.
4	Eine automatische Nummerierung für Folgenummern und IDs muss möglich sein.
5	Die Verknüpfung von Dokumenten mit Objekten muss möglich sein.
6	Das Interface / die GUI muss sich entsprechend der Corporate Identity (CI) des Auftraggebers anpassen lassen.
7	Anpassungen, die im System vorgenommen wurden, müssen beim Update/Upgrade erhalten bleiben und dürfen keine individuellen Nacharbeiten erfordern.

6.21 Reporting Muss-Anforderungen

Nr.	Anforderung
1	Die Erstellung einer unbegrenzten Anzahl an frei definierbaren Reports muss in wenigen, einfachen Schritten möglich sein. Der Bieter hat anzugeben, ob die genutzte Report-Engine selbst entwickelt wurde oder von einem Drittanbieter stammt (z. B. Power BI).
2	Reports müssen mit verschiedenen grafischen Darstellungsoptionen (Diagramme, Tabellen etc.) erstellt werden können.
3	Vorinstallierte Standardreports müssen für jede Funktionalität zur Verfügung stehen.
4	Reports müssen für einzelne Bearbeiter, Bearbeitergruppen oder Rollen hinterlegbar sein.
5	Reports müssen im Self-Service-Portal zugänglich gemacht werden können.
6	Reports müssen automatisierbar sein, z. B. durch automatisierten PDF-Versand per E-Mail.
7	Reports müssen in den Formaten MS Excel und/oder PDF exportiert werden können.

6.22 Rechte- und Rollenmanagement (Plattform) Muss-Anforderungen

Nr.	Anforderung
1	Es muss ein detailliertes Rechtemanagement mit einfacher Vergabe von Rechten an Benutzer geben.
2	Differenzierte Rechteprofile für Entwickler, Administratoren, Helpdesk, IT-Beauftragte und Endnutzer müssen konfigurierbar sein.

6.23 E-Mail-Versand Muss-Anforderungen

Nr.	Anforderung
1	Die Unterstützung von Microsoft Exchange Web Services (EWS) und Exchange Online muss gewährleistet sein.
2	Es muss ein WYSIWYG-Editor zum Erstellen von E-Mail-Templates zur Verfügung stehen.
3	Das automatische Versenden von E-Mails bei Eintreten definierbarer Ereignisse (z. B. Schließen eines Vorgangs) muss möglich sein.

Nr.	Anforderung
4	Das manuelle Versenden von E-Mails direkt aus dem System heraus muss möglich sein.
5	Das Hinterlegen von E-Mail-Templates muss möglich sein.
6	Der Inhalt der E-Mails muss individuell anpassbar sein.
7	Die Einbindung eigener Logos und Grafiken in E-Mails muss möglich sein.

6.24 Benutzeroberfläche (Interface) Muss-Anforderungen

Nr.	Anforderung
1	Es müssen separate Oberflächen bzw. Ansichten für Entwicklung/Programmierung, IT-Nutzer und Self-Service zur Verfügung stehen.
2	Die Benutzeroberfläche muss mehrsprachig sein; primär Deutsch und Englisch müssen unterstützt werden.

**Im Folgenden sind Wunsch-Anforderungen beschrieben.
Das Nicht-Vorhanden sein ist kein Ausschlussgrund. In der Anlage „Fragebogen zur Leistungsbewertung“ muss angegeben werden, ob das Feature vorhanden ist oder nicht. Das Vorhandensein wirkt sich positiv auf die Wertung aus.**

6.25 Active Directory Wunsch-Anforderungen

Nr.	Anforderung
1	Die Software muss automatisch ein Home-Laufwerk für den Benutzer erstellen können. Die Berechtigungsstufe muss einstellbar sein. Der Fileserver muss automatisch auf Basis der Abteilung und/oder des Standorts des Benutzers ausgewählt werden. Eine Laufwerkszuordnung im Active Directory muss konfigurierbar sein.
2	Die Software muss eine grafische Aufbereitung über Active Directory Strukturen (Benutzer ist Mitglied von Gruppe, Gruppe ist Mitglied von Gruppe, Gruppe hat Mitglieder) zur Verfügung stellen. Es ist erforderlich, dass in der Struktur mit einfachen Mitteln (Klick oder ähnliches) navigiert werden kann.
3	Die Software muss sowohl Single- als auch Multi-Domain-fähig sein. Es müssen dabei Domains im gleichen als auch in verschiedenen Forests unterstützt werden.
4	Es muss eine Möglichkeit geben, um Active Directory (und alle anderen Zielsysteme) hinsichtlich ihrer Felder zu konfigurieren. Es muss ein einfach zu konfigurierendes Mapping zwischen Mitarbeiterfeld und Attribut im Active Directory (oder anderem Zielsystem) existieren.
5	Es muss eine Funktion zur Verfügung stehen, die Anomalien im Active Directory und Fileserver analysiert und anzeigt. Mindestens verfügbar sein müssen: Verzeichnisse mit verwaisten SIDs, aufgebrochene Vererbung, Benutzerkonten ohne zeitnahe Anmeldung, leere Gruppen, Benutzer ohne Gruppen, Verzeichnisse mit Berechtigungen 'Jeder' oder 'Authentifizierte Benutzer'.

6.26 Fileserver Wunsch-Anforderungen

Nr.	Anforderung
1	Die Software muss sich regelmäßig mit den Fileservern und den Active Directory Domains abgleichen, damit in der Datenbank der Software immer ein aktueller Datenstand herrscht.
2	Für das Scannen von Fileservern in Standorten mit langsamer Internetverbindung muss die Software eine Beschleunigung, beispielsweise in Form eines Agents, bereitstellen.
3	Für den Fileserver-Report muss es die Möglichkeit geben, Vorgaben anzulegen, sodass ein Bericht mit vordefinierten Optionen mit nur einem Mausklick erzeugt werden kann.
4	Automatisch angelegte Gruppen für Fileserver müssen konfigurierbar aus dem Exchange-Adressbuch ausgeblendet werden können oder auch nicht.

6.27 Helpdesk-Integration Wunsch-Anforderungen

Nr.	Anforderung
1	Die Software muss die Anbindung der Helpdesk-Lösung TOPdesk unterstützen. Es müssen per API-Tickets angelegt werden können, um manuelle Aufgaben im Workflow abzubilden. Die Software muss sich automatisch und regelmäßig über den Ticketstatus synchronisieren. Gilt ein Ticket im Helpdesk als erledigt, so muss dies auch in der Software entsprechend ersichtlich sein.
2	Das Produkt muss die Abarbeitung von manuellen Tätigkeiten unterstützen, die im Rahmen der Workflows angelegt werden. Diese Funktion muss ohne Nutzung eines bestehenden Ticketsystems / Helpdesk-Software angeboten werden.

6.28 Microsoft Teams Wunsch-Anforderungen

Nr.	Anforderung
1	Die Lösung muss in der Lage sein, für ein Team in Microsoft Teams die Besitzer, Mitglieder und Gäste anzuzeigen.
2	Die Software muss für Microsoft Teams anzeigen können, welche Dateien innerhalb eines Teams geteilt werden. Die Lösung muss dabei explizit anzeigen können, welche dieser Dateien mit Personen geteilt werden, die nicht zum Team gehören.

6.29 Passwort-Reset Wunsch-Anforderungen

Nr.	Anforderung
1	Das Portal zum Zurücksetzen des Kennworts soll aus Sicherheitsgründen auf einem anderen Server installierbar sein als der eigentliche Anwendungsserver.
2	Zur Authentifizierung muss das Portal dem Benutzer zusätzlich die Eingabe eines OTP abverlangen. Das OTP wird dabei per Handy über einen SMS-Gateway versendet.
3	Zur Authentifizierung muss das Portal dem Benutzer zusätzlich die Eingabe eines OTP abverlangen. Das OTP wird dabei per Mail an eine alternative Adresse versendet.
4	Zusätzlich zum Active Directory Kennwort müssen auch noch Kennwörter in den anderen integrierten Anwendungen zurückgesetzt werden können.

6.30 PowerShell Wunsch-Anforderungen

Nr.	Anforderung
1	Da mehrere Standorte eingebunden werden, muss die Software unterstützen, dass die Scripts auf konfigurierbaren Agents ausgeführt werden können.
2	Die Software muss dafür sorgen, dass alle relevanten Parameter im Rahmen der Provisionierung automatisch an das Script übergeben werden. Eine manuelle Übergabe von Parametern soll vermieden werden.

6.31 Self Service Wunsch-Anforderungen

Nr.	Anforderung
1	Es muss gesteuert werden können, welche Verzeichnisse am Fileserver für Self Service zur Verfügung stehen.

6.32 Third-Party-Integrationen Wunsch-Anforderungen

Nr.	Anforderung
1	Die Software muss eine offene Schnittstelle zur Verfügung stellen, in der auf Basis einer gängigen Programmiersprache individuelle Anpassungen gemacht werden können. Dabei ist zumindest der Zugriff auf die Schnittstellentechnologien SOAP, REST, LDAP und SQL sicherzustellen.
2	Die Software muss eine Integration mit der Microsoft Remote Desktop Farm (RDS/RDF) ermöglichen. Remote-Anwendungen (RemoteApps) und Desktop-Verbindungen müssen dabei als Ressourcen abbildbar

Nr.	Anforderung
	sein. Im Hintergrund muss die Integration die Mitgliedschaften in den relevanten Active Directory Gruppen automatisch steuern. Der Endanwender darf dabei nicht in Kontakt mit den eigentlichen AD-Gruppenbezeichnungen kommen. Die Konfiguration muss durch den Auftraggeber selbst einfach realisiert werden können.

6.33 Workflows Wunsch-Anforderungen

Nr.	Anforderung
1	Die Software muss eine einfache Oberfläche bieten, mit der Benutzer aus dem Fachbereich neue Mitarbeiter anlegen und bearbeiten können.
2	Im Self Service muss der Fachbereich die Möglichkeit haben, den Zustand/Phase des Mitarbeiters zu bearbeiten. Eine Verschiebung in eine andere Phase (z. B. Elternzeit) muss sowohl sofort als auch zu einem geplanten, zukünftigen Zeitpunkt möglich sein.
3	Die Software muss eine Möglichkeit bieten, ohne Programmierung, den Import von Personendaten aus Vorsystemen (z. B. HR-System) vorzunehmen. Die Software muss dabei Eintritte, Übertritte, sonstige Änderungen und Austritte automatisch erkennen und entsprechend reagieren.
4	Das System muss einen Sicherheitsmechanismus bieten, der ab einem gewissen Prozentsatz an geänderten Datensätzen beim automatischen Import die Verarbeitung verhindert und eine Freigabe erfordert.
5	Beim Import von Personendaten aus Vorsystemen muss es möglich sein, für die Änderung der einzelnen Attribute einen Datumswert zu übermitteln, ab welchem Datum diese Änderung wirksam werden soll (z. B. für geplante Abteilungswechsel).
6	Die Software muss es ermöglichen, dass externe Personen verwaltet werden können. Es muss hierzu eine einfache Oberfläche bereitgestellt werden, die vom Fachbereich bedient werden kann. Die Workflows für externe Personen müssen abweichend zu internen Mitarbeitern konfiguriert werden können.
7	Die zu einem Mitarbeiter zu erfassenden Daten müssen konfigurierbar sein. Es müssen gängige Standardfelder vorgesehen sein. Der Aufbau des Formulars muss frei definierbar sein.
8	Es muss die Möglichkeit geben, eine Genehmigung an eine zentrale Stelle zu eskalieren, wenn ein Antrag über einen bestimmten Zeitraum hinaus nicht beantwortet wird.
9	Es muss die Möglichkeit geboten werden, dass zwischen Beantragung und Provisionierung eines Objekts (eines Mitarbeiters, einer Berechtigung etc.) ein Genehmigungsverfahren geschaltet wird.
10	Genehmigungsworkflows müssen in der Lösung ohne Programmierung gestaltet werden können. Es ist erforderlich, dass ein grafischer Editor zur Gestaltung der Genehmigungsworkflows vorliegt. Dieser muss zumindest folgende Stellen unterstützen: Vorgesetzter, Abteilungsleiter, Dateneigentümer der betroffenen Ressource, IT-Abteilung, Datenschutz und ähnliche.
11	Die Software muss eine qualifizierte, digitale Unterschrift bei Genehmigungsverfahren unterstützen ('eSignature'). Dazu sind zumindest vorzusehen: Windows-Benutzername + Passwort und Microsoft Authenticator Code.
12	Personen, die in einem Workflow eine Aufgabe erhalten, müssen automatisch per E-Mail informiert werden.

6.34 Rezertifizierung Wunsch-Anforderungen

Nr.	Anforderung
1	Die Anwendung muss die Möglichkeit bieten, dass bereits zugeordnete Berechtigungen durch die verantwortlichen Dateneigentümer regelmäßig kontrolliert werden (Rezertifizierung).
2	Für die Rezertifizierung muss es die Möglichkeit geben, die zu kontrollierenden Ressourcen und Personenkreise einzuschränken sowie die Intervalle für die Kontrollen zu definieren. Das System muss die Überprüfung entsprechend dieser Intervalle automatisch anstarten. Die Verantwortlichen sind per E-Mail zu informieren.

6.35 Funktionstrennung (SOD) Wunsch-Anforderungen

Nr.	Anforderung
1	Die Lösung muss eine Möglichkeit für Funktionstrennung (SOD) bieten. Dabei werden bestimmte Objekte miteinander in Konflikt gestellt und dürfen dann nicht oder nur unter Umständen in Kombination bei einem Benutzer zugeordnet sein.

Nr.	Anforderung
2	Die Funktionstrennung muss zumindest Active Directory Gruppen, Microsoft 365-Gruppen, allgemeine Ressourcen und Anwendungsberechtigungen unterstützen.
3	Um die Funktionstrennung einfacher strukturieren zu können, sollen alle Objekte im System mit Tags versehen werden können. Diese Tags müssen anschließend in SOD-Regeln verwendet werden können.
4	Die Funktionstrennung muss zumindest folgende Konsequenzen eines Konflikts unterstützen: strikt verhindern, mit Ausnahme zulassen (per Genehmigung), mit Ausnahme zulassen für einen bestimmten Zeitraum (mit Genehmigung und vorab limitierbarem Zeitraum).
5	Bei der Rücksynchronisation aus angebundenen Fremdsystemen muss die Funktionstrennung auch Konflikte behandeln, die durch eine direkte Berechtigungsänderung im Fremdsystem ausgelöst wurden und nicht über das IAM-System.
6	Die Funktionstrennung muss auf der Benutzeroberfläche in einfacher Art und Weise konfigurierbar sein. Es darf dazu keine individuelle Programmierung erforderlich sein.
7	Der Genehmigungsprozess von Funktionstrennung-Ausnahmen muss konfigurierbar sein und das Vier-Augen-Prinzip ermöglichen.
8	Alle Ausnahmen und Verletzungen der Funktionstrennung müssen protokolliert werden.
9	Nach Anpassung von Funktionstrennungs-Regeln müssen alle bestehenden Berechtigungen anhand der neuen Regeln evaluiert werden können.
10	Die Anforderung von Berechtigungen, die durch Funktionstrennungs-Regeln mit anderen Berechtigungen in Konflikt stehen, muss in der Benutzeroberfläche sofort verhindert werden, sofern konfiguriert ist, dass Ausnahmen nicht zulässig sind.
11	Es muss eine Möglichkeit geben, alle aktuell aktiven Ausnahmen/Akzeptanzen von Funktionstrennungskonflikten anzuzeigen.