A5_GIZ_Whiteboard_Leistungsbeschreibung

Virtuelles Whiteboard als Software-as-a-Service-Lösung (SaaS)

Version 1 vom 23.03.2026

Inhaltsverzeichnis

Abkürzungsverzeichnis

Begriff	Abkürzung
AAD	Azure Active Directory
AG	Auftraggeberin
AN	Auftragnehmer
BHB	Betriebshandbuch
DSGVO	Datenschutz-Grundverordnung
E3/E5	Microsoft 365 (E3/E5)
LLMs	Large Language Models
MA	Mitarbeiter
MDM	Microsoft Intune
MÜ	Maschinelle Übersetzung
SaaS	Software-as-a-Service

1 Einleitung

1.1 Zweck des Dokuments

In der Leistungsbeschreibung sind die Art und der Umfang der zu erbringende Leistung wie auch die dazugehörigen Rahmenbedingungen beschrieben, die Bewerber*innen für die Erstellung eines Angebotes und zur Realisierung der Leistungen benötigen. Die Leistungsbeschreibung wird im Anschluss des Vergabeverfahrens Teil des Vertrags zwischen der Auftraggeberin (AG) und dem Auftragnehmer (AN). Aus der Leistungsbeschreibung gehen die Anforderungen an die einzelnen Positionen im Preisblatt hervor. Außerdem verweist die Leistungsbeschreibung auf ergänzende Anforderungen zur Leistungserbringung, wie zum Beispiel auf Datenschutz- oder Sicherheitsbestimmungen.

1.2 Auftraggeberin

AG ist die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

Als Dienstleisterin der internationalen Zusammenarbeit für nachhaltige Entwicklung und internationale Bildungsarbeit engagiert sich die GIZ weltweit für eine lebenswerte Zukunft. Die GIZ ist hat mehr als 50 Jahre Erfahrung in unterschiedlichsten Feldern, von der Wirtschafts- und Beschäftigungsförderung über Energie- und Umweltthemen bis hin zur Förderung von Frieden und Sicherheit.

Das vielfältige Know-how des Bundesunternehmens GIZ wird rund um den Globus nachgefragt – von der deutschen Bundesregierung, von Institutionen der Europäischen Union, den Vereinten Nationen, der Privatwirtschaft und Regierungen anderer Länder. Wir kooperieren mit Unternehmen, zivilgesellschaftlichen Akteuren und wissenschaftlichen Institutionen und tragen so zu einem erfolgreichen Zusammenspiel von Entwicklungspolitik und weiteren Politik- und Handlungsfeldern bei. Unser Hauptauftraggeber ist das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ).

Alle Auftraggeber*innen und Kooperationspartner*innen schenken der GIZ ihr Vertrauen, Ideen für politische, gesellschaftliche und wirtschaftliche Veränderungen mit ihnen gemeinsam zu entwickeln, konkret zu planen und umzusetzen. Als gemeinnütziges Bundesunternehmen steht die GIZ für deutsche und europäische Werte. Gemeinsam mit den Partner*innen in den nationalen Regierungen weltweit sowie mit Kooperationspartner*innen aus Wirtschaft, Wissenschaft und Zivilgesellschaft arbeitet die GIZ flexibel an wirksamen Lösungen, die Menschen Perspektiven bieten und deren Lebensbedingungen dauerhaft verbessern.

Die GIZ hat zwei Unternehmenssitze in Deutschland: Einen in Bonn und einen in Eschborn bei Frankfurt am Main. Von diesen aus wird das Unternehmen geleitet, wesentliche Teile der fachlichen Arbeit verrichtet und die Auslandstätigkeit der GIZ koordiniert.

1.3 Ausgangslage

Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH ermöglicht durch ihre virtuelle Zusammenarbeit mit Partnern, dass Mitarbeitende, Teams und Organisationseinheiten effektiv und nahtlos in Echtzeit zusammenarbeiten können – unabhängig vom Standort. Dies umfasst Kommunikations-, Interaktions- und Kollaborationstools wie z. B. Live-Chats, Video- und Audiokonferenzen, gemeinsames Dokumentenmanagement, Aufgabenverwaltung, Terminplanung, Brainstorming-Tools wie digitale Whiteboards sowie Projektmanagement-Werkzeuge.

Die Kooperation und Kommunikation mit externen Partner*innen der GIZ soll dadurch verbessert werden. Die Hauptnutzer*innen dieser Lösung sind Mitarbeitende, Teams, Organisationseinheiten und Projekte, gemeinsam mit externen Partner*innen, Kund*innen oder Dienstleister*innen, sofern sie in projektbezogene Aktivitäten eingebunden sind. Ziel ist es, orts- und zeitunabhängig zusammenzuarbeiten, Ideen zu visualisieren, ko-kreativ zu bearbeiten sowie Workshops vorzubereiten und durchzuführen.

Zusätzlich zur bestehenden Infrastruktur ist es entscheidend, ein digitales Whiteboard-Tool zu integrieren, das eine einfache Zusammenarbeit mit externen Partner*innen ermöglicht.

Zu diesem Zweck beabsichtigt die GIZ die Beschaffung von Lizenzen für ein Online-Whiteboard-Tool als SaaS-Lösung, um die virtuelle Zusammenarbeit und das Projektmanagement in verschiedenen Abteilungen und Projekten – insbesondere mit Partnern – zu verbessern. Diese Initiative zielt darauf ab, virtuelle Teamarbeit, Brainstorming und interaktive Sitzungen durch eine leistungsfähige Online-Plattform zu fördern. Das Tool soll sich nahtlos in die IT-Anforderungen hinsichtlich Benutzerfreundlichkeit und Sicherheit integrieren und eine zentrale Oberfläche für Notizen und Aktivitäten vor, während und nach Veranstaltungen bieten.

1.4 Ausstattung der Mitarbeitenden

Alle Mitarbeitenden verfügen über einen Firmenlaptop.

Das Desktop-/Notebook-Betriebssystem bei der GIZ ist derzeit Windows 11 (Version 22H2 oder aktueller). Der Standard-Browser ist Microsoft Edge in der aktuellen Version (Version 127.0.2651.105 oder aktueller), d.h. die SaaS-Lösung muss uneingeschränkt in dieser Microsoft-Umgebung funktionieren.

Die GIZ setzt auf Microsoft 365 (E3/E5) für alle Office- und Kollaborationsanwendungen (z.B. Microsoft Teams, SharePoint, etc.). Verschiedene Dienste werden über Microsoft Azure zur Verfügung gestellt, insbesondere das Azure Active Directory (AAD). Zur Verwaltung der weltweit verteilten Clients wird Microsoft Intune MDM genutzt (derzeit nur bei mobilen Endgeräten). Sämtliche Anwendungen werden mittels Multifaktorauthentifizierung mit Microsoft MFA gesichert.

Aufgrund der weltweiten Präsenz der GIZ sowie der Vielzahl und Heterogenität der Projektländer werden auf mobilen Endgeräten die Betriebssysteme Android und iOS in verschiedenen Versionen eingesetzt. Der Minimumstandard (bei Android 12, bei iOS 16.7.8) für die eingesetzten Versionen wird sich an den Vorgaben von Microsoft Intune orientieren.

1.5 Rollen und Einsatzszenarien

Die Lösung muss die Nutzung durch Projektmitarbeitende, externe Partner*innen sowie interne und externe Dienstleister*innen ermöglichen. Dabei ist sicherzustellen, dass auch externe Personen ohne GIZ-Zugang über geeignete Einladungsmechanismen (z. B. Gastlinks) kollaborativ eingebunden werden können.

Es muss die Möglichkeit bestehen, dass externe Nutzer*innen asynchron auf Whiteboards zugreifen können – insbesondere zur Vorbereitung und Nachbereitung von Inhalten.

Die Lösung soll die kollaborative Arbeit in folgenden typischen Einsatzszenarien unterstützen:

- Zusammenarbeit mit externen Partner*innen (Nicht-GIZ-Mitarbeitende)
- Gemeinsame Entwicklung von Konzepten und Strategien
- Visualisierung und Interaktion in hybriden Meetings
- Einsatz in strukturierten, methodisch geführten Arbeitsprozessen

1.6 Sprache

Die Sprache, in der die Zusammenarbeit erfolgt, ist Deutsch. Dokumente, die zwischen der AG und dem AN ausgetauscht werden, z. B. Dokumentationen oder Betriebshandbücher, sind in deutscher Sprache zu erstellen.

2 Vergabegegenstand

Ziel dieses Auftrags ist die Beschaffung und Bereitstellung eines virtuellen Whiteboards als Software-as-a-Service (SaaS)-Lösung, die es Mitarbeitenden der GIZ ermöglicht, effizient mit externen Partner*innen und Stakeholdern zusammenzuarbeiten.

Die virtuelle Whiteboard-Lösung soll für eine Vielzahl komplexer kollaborativer Anwendungsfälle geeignet sein – darunter, aber nicht ausschließlich: Brainstorming, Planung, konzeptionelle Entwicklung und Co-Creation-Formate.

Der AN ist verantwortlich für die vollständige technische Bereitstellung und den sicheren Betrieb des Systems im Rahmen des SaaS-Angebots. Dies umfasst das Hosting, die Bereitstellung, Wartung, den Support und die allgemeine Pflege der Software über die gesamte Vertragslaufzeit hinweg.

Zur Sicherstellung einer erfolgreichen Implementierung stellt der AN zudem erste Unterstützungsmaßnahmen für Nutzer*innen bereit, darunter ein einmaliges Onboarding für benannte Mitarbeitende der AG (Key User) sowie die Bereitstellung geeigneter Benutzer- und technischer Dokumentation.

Der AN stellt sicher, dass die SaaS-Lösung der AG unverzüglich nach Vertragsbeginn über einen administrativen Nutzerzugang zur Verfügung gestellt wird.

Dieser Zugang muss es den benannten Administrator*innen der AG ermöglichen, unmittelbar mit der Konfiguration und Einrichtung des Systems zu beginnen – ohne zusätzliche Softwareinstallation oder lokale Einrichtung.

Zum Vertragsstart werden 300 Lizenzen (Mindestabnahmemenge) benötigt. Es muss gewährleistet sein das bei Bedarf (auch unterjährig) bis zu 400 weitere Lizenzen hinzugefügt werden können. Bis zu 400 weitere, einzelne Lizenzen sollen demzufolge bei Bedarf abgerufen werden können.

2.1 Funktionale und technische Anforderungen an die SaaS-Lösung

Die in der folgenden Tabelle aufgeführten Anforderungen sind in der Spalte „Kriterium“ als „Muss“ oder „Soll“ gekennzeichnet. Der Bieter hat in der Anlage „B4_GIZ_Whiteboard_Kriterienkatalog je Kriterium anzugeben, ob er die Anforderung erfüllt.

Kategorie	Lfd. Nr.	Anforderung	Kriterium
Nutzergruppen und Einsatzszenarien	2.1.1	Das Tool ermöglicht eine Nutzung durch Projektmitarbeitende, externe Partner*innen und Dienstleister (intern/extern).	Muss
	2.1.2	Es besteht die Möglichkeit des asynchronen Zugriffs von Externen für die Vor- bzw. Nachbereitung von Whiteboards.	Muss
	2.1.3	Die Lösung soll die kollaborative Arbeit in folgenden typischen Einsatzszenarien unterstützen: ▪ Zusammenarbeit mit externen Partner*innen (Nicht-GIZ-Mitarbeitende) ▪ Gemeinsame Entwicklung von Konzepten und Strategien	Muss

		▪ Visualisierung und Interaktion in hybriden Meetings ▪ Einsatz in strukturierten, methodisch geführten Arbeitsprozessen	
Anforderungen an die Bedienung	2.1.4	Das Tool ermöglicht die Verwaltung und Nutzung von Templates und Vorlagen in einer Bibliothek	Muss
	2.1.5	Die Bibliothek beinhaltet Standard-Vorlagen für Brain-storming, Projektmanagement, Team-Kollaboration, Strategieworkshops, Agile Methodiken etc.	Soll
	2.1.6	Das Tool beinhaltet eine Voting- bzw. Abstimmungsfunktion.	Soll
	2.1.7	Rollen und Berechtigungen (Bearbeiter, Moderator, etc.) können vom Board-Admin jederzeit angepasst werden.	Muss
	2.1.8	Das Tool bietet Navigationsmöglichkeiten, um auch bei großen Boards Übersichtlichkeit zu gewährleisten (z.B. Arbeiten mit Board-Abschnitten, Minimap).	Soll
	2.1.9	Das Tool besitzt eine Funktion zum Einfügen von Kommentaren.	Soll
	2.1.10	Das Tool beinhaltet eine Funktion zum Einfügen und Bearbeitung von Tabellen	Soll
	2.1.11	Das Tool besitzt eine Suchfunktion für Inhalte auf dem Board.	Soll
	2.1.12	Das Tool besitzt eine Möglichkeit zur Zeitsteuerung (Timer-Funktion).	Soll
	2.1.13	Das Tool besitzt Möglichkeiten zum Aufgabenmanagement (Mindestens Zuweisung von Aufgaben).	Soll
	2.1.14	Die Oberfläche des Tools muss auf Deutsch und Englisch verfügbar sein.	Muss

	2.1.15	Die Oberfläche des Tools soll auf Französisch verfügbar sein.	Soll
	2.1.16	Die Oberfläche des Tools soll auf Spanisch verfügbar sein.	Soll
	2.1.17	Das Tool beinhaltet Drag-and-Drop Funktionen (z.B. für Bilder).	Soll
	2.1.18	Das Tool beinhaltet eine Möglichkeit zum Export von Boardinhalten in gängige Formate (mindestens als PDF und als Bilddatei).	Muss
	2.1.19	Das Tool soll den Anforderungen der Barrierefreiheit gemäß EN 301 549 und BITV 2.0 entsprechen. Es sollte vollständig mit Tastatur bedienbar sein, Screenreader unterstützen und für Menschen mit Seh-, Hör- oder motorischen Einschränkungen nutzbar sein.	Soll
Übergreifende Anforderungen	2.1.20	Das Tool beinhaltet Single Sign-On (SSO) via Entra-ID (SAML 2.0) zwecks Lizenzverwaltung und Authentifizierung.	Muss
	2.1.21	Das Tool verfügt über eine automatisierte Löschung/Deaktivierung des Users im System, bei abgelaufener Lizenzen.	Soll
	2.1.22	Das Tool muss über die gängigen Web-Browser (Mindestens Chrome, Edge, Firefox) nutzbar sein.	Muss
	2.1.23	Das Tool beinhaltet die Möglichkeit eines einfachen Zugangs für Externe und Gäste ohne Account-Registrierung, mithilfe von Einladungslinks.	Muss
	2.1.24	Das Tool muss das kollaborierte Arbeiten mit vielen gleichzeitigen Nutzer*innen (mindestens 30) ermöglichen.	Muss
	2.1.25	Das Tool beinhaltet Optionen zur Wahl von Modi für die Bedienung mit diverser Hardware (Touch-Screen, Maus, Trackpad).	Soll

Sicherheits- und Datenschutzanforderungen	2.1.26	Das Tool muss den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen.	Muss
	2.1.27	Der Serverstandort der angebotenen Lösung muss sich innerhalb des Europäischen Wirtschaftsraums (EWR) befinden.	Muss
	2.1.28	Das Tool muss über einen Passwortschutz für Whiteboards und gespeicherte Inhalte verfügen.	Muss
	2.1.29	Das Tool muss eine durchgehende verschlüsselte Datenübertragung (z. B. TLS) gewährleisten.	Muss

2.2 Nicht-funktionale Anforderungen

Die GIZ betreibt ein Informationssicherheits-Managementsystem (ISMS) und plant eine Zertifizierung gemäß ISO/IEC 27001 sowie die Aufrechterhaltung dieses Zertifikats. Im Rahmen der Zertifizierung wird die aktuelle Version des genannten Standards umgesetzt.

Folgende Regelungen zur Informationssicherheit finden bei der Leistungserbringung Anwendung:

2.2.1 Mindestanforderungen an Authentisierungsmittel/Passwörter

Der AN muss mindestens folgende Anforderungen an die Passwortqualität für alle Accounts, mit denen auf GIZ-Informationen zugegriffen wird/werden kann, umsetzen:

- Passwörter müssen mindestens 10 Zeichen lang sein, für privilegierte Konten mindestens 16 Zeichen
- Passwörter für technische Konten müssen mindestens 20 Zeichen lang sein, sofern ein regelmäßiger Passwortwechsel (z.B. über Managed Service Accounts) nicht gewährleistet werden kann
- Das Passwort muss sich aus 3 der 4 folgenden Merkmale zusammenzusetzen: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis z), Ziffern (0 bis 9) und Sonderzeichen (zum Beispiel: !, $, #, %)
- Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden.
- Passwörter dürfen nicht identisch zu einem der letzten 10 benutzten Passwörter sein.
- Passwörter müssen regelmäßig geändert werden.

Für Konten mit administrativen Berechtigungen muss eine Multi-Faktor-Authentifizierung (mindestens zwei Faktoren) genutzt werden.

2.2.2 Zertifikatsfehler bei Nutzern

Es muss gewährleistet sein, dass bei der Nutzung von Zertifikaten, keine Zertifikatsfehler auftreten.

2.2.3 Mindestanforderungen an die Datensicherung

Der AN muss folgende Anforderungen an das Verfahren für die Datensicherung für die verarbeiteten Daten erfüllen:

- Aus der Datensicherung müssen sich die für die bereitgestellte Leistung notwendigen technischen Komponenten/Anwendungen entsprechend der aufgeführten Parameter vollständig wiederherstellen lassen:
  - Die Häufigkeit der Datensicherung ist (RPO/maximal zulässiger Datenverlust): mindestens 7 Tage
  - Die Wiederherstellung aller technischen Komponenten/Anwendungen beträgt (RTO/geforderte Wiederanlaufzeit): höchstens 48 Stunden
  - Die Aufbewahrungszeit für die Datensicherungen beträgt: mindestens 21 Tage
- Die technischen Komponenten und der Ort der Speicherung der Datensicherung müssen sich mindestens in zwei unterschiedlichen Brandabschnitten befinden.

2.2.4 Leistungskennzahlen

Während der gesamten Projektlaufzeit muss auf Anforderung der AG ein Bericht (maximal halbjährlich) zur Informationssicherheit zur Verfügung gestellt werden, über deren Inhalt sich AG und AN abstimmen.

Bei Nichteinhaltung der beschriebenen Leistungskennzahlen (vgl. Verfügbarkeitsklasse VK1 im EVB-IT Cloud-AGB) kann die AG nach den gesetzlichen Regelungen Schadensersatz geltend machen oder die Vergütung mindern.

2.2.5 ISMS des Auftragnehmers

Der AN muss über ein angemessenes, dokumentiertes und implementiertes Informations-Sicherheits-Management-System (ISMS) verfügen, das dem Standard ISO/IEC 27001:2022 (bzw. aktuelle Folgeversionen) oder vergleichbar entspricht. Das ISMS muss die zu erbringende Leistung inklusive der verarbeitenden Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfassen.

Der AN muss eine/n Informationssicherheitsbeauftragte/n (Chief Information Security Officer) benennen, welche/r über die erforderliche Fachkunde verfügt und teilt der AG dessen/deren Kontaktdaten auf Anforderung mit.

Die AG wird einen Kontakt als ausschließliche/n Ansprechpartner/in in allen Fragen des AN bezüglich der Informationssicherheit benennen.

2.2.6 Benutzermanagement

Das ISMS des AN muss Verfahren zur dokumentierten Vergabe, Änderung, Sperrung, Entsperrung, Deaktivierung und Reaktivierung von (privilegierten, internen, externen und anderen) Benutzerkonten sowie zur zweifelsfreien Identifikation berechtigter Personen und zur Rücksetzung von Passwörtern beinhalten.

Diese Verfahren müssen technische Maßnahmen zum Schutz vor Brute-Force Angriffen (z.B. Sperrung von Benutzeraccounts nach mehrmaliger fehlerhafter Authentisierung) beinhalten.

Der AN muss im Rahmen seines ISMS für das Benutzermanagement folgendes sicherstellen:

- Benutzerkennungen müssen deaktiviert werden, wenn sie nicht mehr oder für mehr als 6 Monate nicht mehr benötigt werden.
- Benutzerkennungen dürfen nur gelöscht werden, wenn durch die Löschung keine Gefahr besteht, dass vorhandene Protokolle, Logdateien oder sonstige Aufzeichnungen innerhalb des Archivierungszeitraums nicht mehr eindeutig einer Person zugeordnet werden können.
- Werden nicht-personalisierte Benutzerkonten (z.B. root-Account, Benutzerkonten für den IT-Notfall) eingesetzt, so muss durch geeignete Maßnahmen sichergestellt werden, dass die mit diesem Konto durchgeführten Aktivitäten jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zugeordnet werden können.
- Technische Benutzerkonten dürfen ausschließlich von Services oder Skripten benutzt werden. Die Nutzung des Kontos darf nicht durch eine Person erfolgen.
- Technische Benutzerkonten dürfen nur mit minimalen Berechtigungen entsprechend dem Berechtigungskonzept konfiguriert werden. Es muss das „Least-Privilege“ Prinzip umgesetzt werden.
- Privilegierte Benutzerkonten dürfen ausschließlich für administrative Tätigkeiten benutzt werden.
- Privilegierte Benutzerkonten für externe Benutzer*innen müssen auf maximal 6 Monate befristet eingerichtet werden und können bei Bedarf nach Ablauf verlängert werden.
- Benutzerkonten für externe Benutzer*innen dürfen nur befristet, jedoch maximal für ein Jahr vergeben werden. Die Befristung muss sich an der Vertragslaufzeit der extern nutzenden Person orientieren. Accounts können ggf. aktiv erneuert werden.

Der AN muss sicherstellen, dass administrative Tätigkeiten nur über personalisierte Konten durchgeführt werden und dass diese Konten ausschließlich für administrative Zwecke genutzt werden.

2.2.7 Berechtigungsmanagement

Das ISMS des AN muss ein dokumentiertes Verfahren zur dokumentierten Genehmigung, Vergabe, Änderung, Korrektur, regelmäßigen Aktualisierung und dem zeitnahen Entzug von Berechtigungen enthalten.

Die Berechtigungskonzepte des AN müssen auf den Prinzipien "Need-to-know" und "Least-Privilege " basieren und wirksam durchgesetzt sein.

Im Rahmen des Berechtigungsmanagements müssen die Anforderungen an die Funktionstrennung (Segregation of Duties) umgesetzt werden.

Das Berechtigungskonzept muss technische und organisatorische Maßnahmen beinhalten, welche die Wirksamkeit des Berechtigungskonzepts sicherstellen.

2.2.8 Change- und Patchmanagement

Das ISMS des AN muss Verfahren für das Test-, Change- und Patchmanagement in Anlehnung an gängige Standards (z.B. ITIL) beinhalten, dass die sichere, regelmäßige (mindestens alle 6 Monate) und anlassbezogen unverzügliche Implementierung von (Sicherheit-)Patches und Updates für die bereitgestellte Leistung gewährleistet.

2.2.9 Trennung von Test- und Produktionsumgebungen

Durch das ISMS des AN und technische Maßnahmen muss sichergestellt sein, dass Schwachstellen, Bedienfehler oder technische Fehler in Testumgebungen kein Risiko für die Produktivumgebung darstellen (z.B. durch Trennung von Testumgebung und Produktionsumgebung durch eine Firewall).

Testumgebungen müssen im Wesentlichen den zugehörigen Produktivumgebungen entsprechen."

2.2.10 Management von Sicherheitsvorfällen

Der Prozess zur Erkennung, Priorisierung, Behandlung und Dokumentation von Sicherheitsvorfällen (Security Incidents) und anderen Störungen muss die zentrale Erfassung und Auswertungen von relevanten Loginformationen beinhalten.

2.2.11 Schwachstellenmanagement

Der AN muss ein Verfahren zur Erkennung, Bewertung (z.B. CVSS), Priorisierung, Beseitigung und Dokumentation von Schwachstellen für die bereitgestellte Leistung umsetzen.

Der AN muss an die AG quartalsweise über die für die zu erbringende Leistung relevanten erkannten Schwachstellen, sowie deren Bewertung und Beseitigung berichten.

Der AN muss ein Verfahren für regelmäßige (mindestens jährlich), automatisierte und protokollierte Schwachstellenscans umsetzen.

2.2.12 Härtungskonzept

Der AN muss ein Verfahren zur Härtung der technischen Komponenten umsetzen. Das Verfahren muss insbesondere sicherstellen, dass

- nicht benötigte oder unerwünschte Dienste oder Schnittstellen deaktiviert sind,
- nicht benötigte Benutzerkennungen deaktiviert oder gelöscht sind und
- voreingestellte Passwörter geändert werden.

2.2.13 Interne Audits

Der AN muss ein Verfahren umsetzen, das sowohl regelmäßige als auch anlassbezogene Prüfungen der Sicherheitsmaßnahmen auf Angemessenheit und Wirksamkeit (wie zum Beispiel Soll-Ist-Vergleiche von Konfigurationen, Firewall-Regelwerken oder Penetrationstests) beinhaltet und die Prüfergebnisse protokolliert.

2.2.14 Arbeitsplätze von Administratoren

Der AN stellt sicher, dass der Zugang zu Systemen zu Administrationszwecken nur von gehärteten, zugangsbeschränkten und überwachten Arbeitsplätzen erfolgen kann.

2.2.15 Schutz vor Schadsoftware

Der AN muss ein Verfahren zum kontinuierlichen Schutz technischer Komponenten vor Schadsoftware und ein Reaktionskonzept für großflächig auftretende Schadsoftware (z.B. Ransomware) umsetzen.

2.2.16 Datensicherungskonzept

Der AN muss ein Verfahren für die Datensicherung umsetzen, das regelmäßige und dokumentierte Tests der Wiederherstellung von Datensicherungen beinhaltet.

2.2.17 Mandantentrennung

Der AN muss ein technisches Verfahren zur Mandantentrennung umsetzen, das sicherstellt, dass Informationen und Verarbeitungskontexte verschiedener Kunden getrennt gehalten werden.

2.2.18 Umgang mit Authentisierungsmitteln

Der AN muss ein Verfahren zur Verwendung, zum sicheren Wechsel, Austausch, Speichern und Hinterlegen von Authentisierungsmitteln (z.B. Passwörtern), sowie eine Regelung zum sicheren Umgang mit Authentisierungsmitteln (z.B. Passwörtern) umsetzen.

Der Missbrauch von Authentisierungsmitteln muss als Sicherheitsvorfall bewertet und behandelt werden.

2.2.19 Löschkonzept

Der AN muss ein Verfahren für die Rückgabe, das vollständige Löschen (d.h. nicht rekonstruierbar) und das Vernichten von Daten umsetzen, so dass von der Aufraggeberin als „nicht mehr benötigt“ klassifizierte Daten umgehend gelöscht werden, sofern sie keiner gesetzlichen oder vertraglichen Aufbewahrungs- oder Sperrfrist unterliegen und eine Löschung mit technisch vertretbarem Aufwand möglich ist.

Insbesondere muss dieses Verfahren Anwendung finden für Informationen der Auftraggeberin bei der geplanten oder ungeplanten Beendigung der Leistungserbringung.

Die Löschung ist der Auftraggeberin auf Verlangen und durch entsprechende Erklärung oder anderweitig nachzuweisen. Das Löschverfahren muss auf Anforderung nachgewiesen werden.

2.2.20 Sicherer Betrieb von Firewalls

Der AN muss durch ein geeignetes Verfahren sicherstellen, dass alle Firewalls mit einem minimalen Regelwerk (Whitelisting) betrieben werden.

Die Regelwerke müssen dokumentiert sein und der IST-Stand der Regelwerkskonfiguration der Firewalls muss regelmäßig mit dem dokumentierten SOLL-Zustand verglichen werden.

2.2.21 Einsatz von Kryptographie – Kryptokonzept

Der AN muss ein Verfahren umsetzen, das den wirksamen Gebrauch von Kryptographie und das Schlüsselmanagement zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen beinhaltet.

Der AN muss bei Übertragung und Speicherung von Daten der Auftraggeberin eine angemessene Verschlüsselung sicherstellen (d.h. sowohl "In Transit" als auch "At Rest").

Insbesondere die Kommunikation über nicht vertrauenswürdige Verbindungen (z.B. WAN, Internet) muss angemessen verschlüsselt erfolgen.

Die Verschlüsselungsprotokolle und -verfahren des AN müssen dem aktuellen Stand der Technik entsprechen.

2.2.22 IT-Notfallmanagement

Der AN muss über ein angemessenes, dokumentiertes und implementiertes IT-Notfallmanagement verfügen, welches die zu erbringende Leistung inklusive der verarbeitenden

Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfasst.

Das IT-Notfallmanagement des AN muss einem kontinuierlichen Verbesserungsprozess unterliegen.

Das IT-Notfallmanagement muss mindestens die folgenden Szenarien beinhalten:

- Ausfall eines Gebäudes
- Ausfall eines Rechenzentrums
- Ausfall von Kommunikationsinfrastruktur

Notfalltests für diese Szenarien müssen regelmäßig durchgeführt und dokumentiert werden. Die Ergebnisse der Notfalltests müssen zur Verbesserung genutzt werden.

2.3 Self-paced Schulungspaket

Der AN stellt ein umfassendes Self-paced Schulungspaket zur Verfügung, das den Anwendern eine eigenständige Einarbeitung in die Whiteboard-SaaS-Anwendung ermöglicht. Dieses Paket umfasst insbesondere:

- Geeigneten Schulungsressourcen (z.B. Videotutorials, Knowledge Base, Anleitungen etc.) mind. in den Sprachen Deutsch und Englisch zur schrittweisen Einführung in die Funktionen und Anwendungsszenarien der Whiteboard-Lösung.
- Die Unterlagen sind so zu konzipieren, dass sie sowohl neuen als auch erfahrenen Anwendern eine effektive Nutzung der Anwendung ermöglichen.
- Der Aufwand für die Erstellung der Schulungsunterlagen ist durch den AN zu schätzen und im Preisblatt als Pauschal-Festpreis auszuweisen.

Ziel ist es, den Nutzenden eine flexible, zeit- und ortsunabhängige Schulung zu ermöglichen, die den produktiven Einsatz der Anwendung ohne zusätzliche Präsenzschulungen sicherstellt.

2.4 Initiale Dienstleistungen/Beratung zur Einrichtung der SaaS-Lösung und Einrichtung der Rollen und Berechtigungen

Der AN unterstützt die AG bei der Erstkonfiguration der Whiteboard-SaaS-Anwendung. Dies umfasst:

- Beratung zur optimalen Einrichtung der Anwendung gemäß den Anforderungen des Auftraggebers.
- Einrichtung und Dokumentation von Rollen und Berechtigungen für ausgewählte Nutzergruppen (z. B. Administratoren, Fachanwender, Key-User).
- Unterstützung bei der technischen Inbetriebnahme
- Abstimmung mit relevanten internen Stakeholdern zur Integration in bestehende Systeme und Prozesse.

- Einmaliges Onboarding für benannte Mitarbeitende der AG (Key User)
- Mitwirkungsleistungen bei Erstellung des Betriebshandbuchs (Bereitstellung techn. Informationen zur Anwendung, Dokumentation relevanter Konfigurations- und Administrationsprozesse, Abstimmung der Inhalte mit dem Auftraggeber zur Integration in ein einheitliches Betriebshandbuch)

2.5 Optionale Dienstleistungen

Bei Bedarf können während der Vertragslaufzeit optionale Beratungs- und Programmierleistungen u.a. zu folgenden Punkten abgerufen werden:

- Datenmigration
- Einrichtung von Rollen und Berechtigungen
- Workflows
- Integration in bestehende Systeme
- Unterstützung bei der Behebung von Problemen und Durchführung von Optimierungen
- Unterstützungsleistungen bei Release-Wechsel
- Unterstützungsleistungen bei der Aktualisierung der Dokumentation (Betriebshandbuch, Benutzerhandbuch, Schulungsunterlagen für Endnutzende)
- Weitere Customizing-Leistungen, falls Bedarf besteht.
- Datenexport zu Vertragsende: Der AN stellt sicher, dass zum Vertragsende ein vollständiger und strukturierter Export aller Inhalte (insbesondere Boards und zugehörige Daten) erfolgt. Dies umfasst:
    - Prüfung der Datenbestände auf Vollständigkeit und Exportfähigkeit,
    - Migration verbleibender Daten in ein vereinbartes Zielformat zur weiteren Nutzung durch die AG.
    - Der Export muss nachvollziehbar dokumentiert und technisch abgesichert erfolgen

Hierzu ist im Preisblatt unter Position 5.1 ein entsprechender Preis zu hinterlegen. Eine vertragliche Verpflichtung zur Abnahme dieser Leistung besteht nicht.