Service Level Agreement

Archive-IT - SaaS

Datum	**30. November 2021**
Version	**1.2**

smart. safe. solid.

Inhaltsverzeichnis

Versiehistorie

Autor	Version	Datum	Änderung(en)
Roy Peeters	Concept	02-07-2018	
Hein Boots	1.0	09-05-2019	Ergänzungen nach gegenseitigen Konsultationen
Roy Peeters	1.1	26-03-2021	Anpassungen lieferbare Ergebnisse
Roy Peeters	1.2	30-11-2021	Geringfügige textliche Änderungen

1. Allgemein

1.1 Einführung

In diesem Service Level Agreement (SLA) werden die Service-Levels von Archive-IT in Bezug auf SaaS-Software detailliert beschrieben/erklärt.

1.2 Begriffe und Definitionen

Großgeschriebene Begriffe, die in diesem SLA verwendet werden, haben die im nachstehenden Glossar festgelegte Bedeutung oder, falls sie dort nicht aufgeführt sind, die Bedeutung, die ihnen in einem der anderen Teile der Vereinbarung gegeben wird:

Konzept	Definition
Abteilung Unterstützung	Die Support-Abteilung von Archive-IT.
Verwaltung	Die proaktive, reaktive und adaptive Verwaltung des SaaS-Dienstes mit dem Ziel seiner Verfügbarkeit und Kontinuität. Dazu gehört auch die Implementierung von Patches, neuen Versionen und neuen Versionen der zugrunde liegenden Anwendungen und Systemsoftware.
Verfügbarkeit	Der Verfügbarkeitsstandard des SaaS-Dienstes wird als Prozentsatz der Zeit angegeben, in der der SaaS-Dienst während des Servicefensters genutzt werden kann. Formel: [(Dienstfenster - Ausfallzeit)/ Dienst (Fenster)] X 100% Unter Verfügbarkeit ist die technische Möglichkeit zu verstehen, sich in das Portal von Archive-IT einzuloggen, das den Zugang zum SaaS-Dienst ermöglicht und die vereinbarte Funktionalität bereitstellt.
Change	Eine Änderung/Modifikation (eines Teils) des SAAS-Dienstes.
Change Advisory Board (CAB)	Die Verantwortlichen für die Genehmigung von RFCs-Anfragen.
Change Manager	Endgültige Verantwortung des Change Advisory Board.
Downtime	Zeitraum, in dem der SaaS-Dienst innerhalb des Service-Fensters nicht verfügbar ist.
Vorfall	Betriebliches Ereignis, das nicht zum Standardbetrieb des SaaS-Dienstes gehört und zu einer Beeinträchtigung des vereinbarten Betriebsdienstes führt.
Benachrichtigung	Allgemeine Fragen, Bitten und Beschwerden, die keinen Vorfall darstellen.
Wartung	Durchführung von korrigierenden, adaptiven oder präventiven Wartungsarbeiten.

	Dazu gehören regelmäßige Aktualisierungen der Umgebung und der Software (Firewall-Updates, Sicherheits-Patches, Betriebssystem usw.).
Wartungsfenster	Der Zeitraum, in dem Archive-IT (a) planmäßige Wartungsarbeiten durchführt und (b) notwendige zusätzliche Wartungsarbeiten durchführt, für die kein Aufschub möglich ist (denken Sie an Sicherheitsrisiken usw.).
Auflösungszeit	Die Anzahl der Arbeitsstunden zwischen dem Zeitpunkt der Bearbeitung eines Vorfalls und der Lösung des Vorfalls.
Patch of Fix	Eine Änderung der zugrunde liegenden Anwendung(en) oder Systemsoftware, um Fehler zu beheben.
Problem	Eine unerwünschte Situation, die aus verwandten Vorfällen identifiziert wurde und deren Ursache noch nicht bekannt ist.
Reaktionszeit	Die Zeit, die zwischen der Meldung des Vorfalls durch den Kunden gemäß der vereinbarten Meldemethode und dem Zeitpunkt der Bearbeitung der Meldung durch Archive-IT vergeht.
RFC – Request for Change	Ein RFC ist ein Synonym für ein Change Ticket. Ein Antrag auf Änderung (einer Komponente) des SaaS-Dienstes.
Service-Fenster	Zeitraum, in dem der SaaS-Dienst erbracht wird, abzüglich des Wartungsfensters.
Arbeitstage	Montag bis Freitag mit Ausnahme der nationalen (niederländischen) anerkannten Feiertage (wie auf der Website der Zentralregierung angegeben).
Arbeitszeiten	Von 08:15 bis 17:00 Uhr an Werktagen.
Workaround	Eine vorübergehende Lösung für einen Vorfall.

2. Software

2.1 Vorfälle/Berichte einreichen

Bei Vorfällen/Berichten im Zusammenhang mit der Archive-IT-Software wenden Sie sich bitte über das sichere **Online-Support-Portal** an die Support-Abteilung. Vorfälle/Berichte können rund um die Uhr registriert werden. In diesem Online-Support-Portal können Sie auch den Fortschritt und den Verlauf Ihrer Vorfälle/Meldungen einsehen.

Haben Sie noch keinen Zugang dazu? Dann können Sie es unter support@archive-it.de anfordern.

2.1.1 Erreichbarkeit des Support Desks

Die Support-Abteilung überwacht den Fortschritt und das Feedback zu den Vorfällen/Berichten. Die Support-Abteilung ist an normalen Arbeitstagen zwischen 8.15 und 17.00 Uhr zu erreichen. An Wochenenden und Feiertagen ist kein Personal anwesend.

In besonders dringenden Fällen kann ein Vorfall auch telefonisch gemeldet/geklärt werden (an normalen Arbeitstagen/Arbeitszeiten). Die Support-Abteilung ist unter der Telefonnummer +31 77 750 11 00 zu erreichen.

Archive-IT ist bestrebt, Incidents innerhalb der festgelegten Lösungszeiten zu lösen (siehe Abschnitt Reaktions- und Lösungszeiten).

2.1.2 Management von Zwischenfällen

Die folgenden Schritte werden nach Erhalt eines Vorfalls/einer Meldung durchgeführt:

- Klassifizierung und Prioritätensetzung.
- Überwachung des Fortschritts bis zur endgültigen Freigabe.
- Übermittlung von Statusinformationen.
- Behandlung von Vorfällen/Benachrichtigungen.

Ein Vorfall kann zu einem Request For Change (RFC) führen.
Vorfälle/Benachrichtigungen können zu einem RFC führen. Der Vorfall/Bericht wird dann vorübergehend auf Eis gelegt - mit einem Hinweis auf den RFC. Bei hoher Dringlichkeit kann beschlossen werden, innerhalb der festgelegten Lösungszeit eine Umgehung oder Behebung vorzuschlagen.

2.1.3 Reaktions- und Lösungszeiten

Die Reaktions- und Lösungszeiten werden auf der Grundlage der angegebenen Auswirkungen und der Klassifizierung festgelegt. Die Kombination dieser beiden Faktoren bestimmt die Priorität.

Festlegung eines Wirkungscodes

Aufschlagcode	Ausmaß des Vorfalls
Hoch	Mehr als 10 Benutzer oder geschäftskritische Prozesse
Mittel	2-10 Benutzer
Niedrig	1 Benutzer

Festlegung der Klassifizierung von Vorfällen

Aufschlagcode	Folgen des Vorfalls
Hoch	Ein Durcharbeiten ist nicht möglich oder es beeinträchtigt geschäftskritische Prozesse
Mittel	Durcharbeiten ist schwierig
Niedrig	Durcharbeiten ist möglich

Prioritätensetzung

Die Kombination aus **Impact Code** und **Klassifizierung** bestimmt die Priorität eines Incidents.

Priorität Klassifizierung			
Aufschlagcode	**Hoch** **(Durcharbeiten nicht möglich)**	**Mittel** **(Durcharbeiten ist schwierig)**	**Niedrig** **(Durcharbeiten ist möglich)**
Hoch (>10 Benutzer)	I	I	II
Mittel (2-10 Benutzer)	I	II	III
Niedrig (1 Benutzer)	III	III	III

Ermittlung der Dringlichkeit

Je nach Priorität wird die Dringlichkeit gemäß der nachstehenden Matrix festgelegt.

Entladung und Reaktionszeit		
Priorität	**Reaktionszeit**	**Auflösungszeit**
I (dringend)	< 1 Arbeitstag	< 1 Arbeitstag
II (weniger dringend)	< 1 Arbeitstag	< 1 Arbeitswoche
III (nicht dringend)	< 1 Arbeitstag	< 1 Monat

Archive-IT wird auch dann, wenn die Ursache des Vorfalls nicht auf Archive-IT zurückzuführen ist, alle Anstrengungen unternehmen, um den Vorfall zu lösen. Archive-IT wendet jedoch keine "Lösungszeiten" für solche Vorfälle an. Archive-IT ist berechtigt, für die in diesem Zusammenhang erbrachten Leistungen ein Honorar nach den üblichen Sätzen zu berechnen.

2.1.4 Berichte über Vorfälle/Berichte

Über das Online-Supportportal können Sie die folgenden Probleme melden:

- Die Anzahl der Vorfälle.
- Pro Vorfall die "Lösungszeit" und "Reaktionszeit".
- Die Anzahl der Vorfälle, gruppiert nach Priorität.
- Eine Liste der offenen Vorfälle und RFCs.

2.2 Geplante Wartung

Die planmäßige Wartung des SaaS-Dienstes findet außerhalb der Arbeitszeiten/Arbeitstage während des Wartungsfensters statt.

Wartung auf der Ebene des Betriebssystems und der Infrastruktur

Wartung auf der Ebene des Betriebssystems und der Infrastruktur
Dies betrifft (Sicherheits-)Updates auf Betriebssystemebene (Windows-Updates) und mögliche Wartungsarbeiten auf Infrastrukturebene, die von unserem Hosting-Partner durchgeführt werden. Eine Woche vor der Freigabe in den Produktionsumgebungen testet Archive-IT diese Wartung zunächst ausgiebig in der Abnahmeumgebung. Sollten (erwartete) Probleme auftreten, wird die Einführung in den Archive-IT-Produktionsumgebungen verschoben.

In der Regel findet diese Wartung am Mittwochabend/nachts zwischen 20:00 und 01:00 Uhr statt. Pro Jahr sind etwa 13 Wartungstermine vorgesehen, die rechtzeitig, jedoch mindestens 4 Arbeitstage im Voraus angekündigt werden.

Archive-IT Software-Wartung

Während der regulären Wartung der Archive-IT Software ist die Verfügbarkeit nicht gefährdet (außer in Ausnahmefällen, in denen Archive-IT Sie sofort informiert), da die SaaS-Architektur der Archive-IT Software und der Umbrella-Rollout-Mechanismus einen Rollout ohne Auswirkungen auf die Verfügbarkeit berücksichtigen. Sollte dennoch ein Problem auftreten, ist es einfach, innerhalb kurzer Zeit zu einer früheren Version zurückzukehren.

Solche Wartungsarbeiten - soweit erforderlich oder notwendig - finden außerhalb der Arbeitszeit statt und sind rechtzeitig, mindestens jedoch 4 Arbeitstage im Voraus, anzukündigen.

2.3 Change- und Release-Management

Anträge auf Änderungen an der Software sollten ebenfalls über das Online-Supportportal gestellt werden. Archive-IT prüft die vorgeschlagene Änderung auf ihre Durchführbarkeit und ihre Folgen (einschließlich der Kosten) und entscheidet, ob und in welchem Umfang die vorgeschlagene Änderung umgesetzt wird. Ein nicht genehmigter Änderungsantrag wird von Archive-IT mit Begründung abgelehnt.

Für wichtige Aktualisierungen werden Versionshinweise erstellt.

2.4 Escrow-Software

Die Parteien legen Wert auf Kontinuität, was die Software und die gehosteten Daten anbelangt. Archive-IT ist die richtige Adresse dafür. Wenn Sie noch mehr Sicherheit wünschen: Archive-IT hat einen zuverlässigen Partner gefunden, der eine solide Escrow-Einrichtung anbieten kann. Wenn Sie daran interessiert sind, wenden Sie sich bitte an Archive-IT, um weitere Einzelheiten über Escrow zu erfahren.

2.5 Dienstleistungsparameter SaaS

2.5.1 Verfügbarkeit

Der SaaS-Dienst wird innerhalb einer Plattform von Infrastructure-as-a-Service-Diensten bereitgestellt und mit einer Verfügbarkeitsgarantie* von 99,9 % angeboten. Dies geschieht in Zusammenarbeit mit dem Rechenzentrumspartner aus Rechenzentren in den Niederlanden.

* In diesem Zusammenhang bedeutet "**nicht verfügbar**", dass es für alle Benutzer nicht verfügbar ist (vollständige Nichtverfügbarkeit).

Die zugrunde liegende Infrastruktur erfüllt hohe Sicherheitsanforderungen, hohe Verfügbarkeit und Redundanz aller primären Einrichtungen. Alle Daten und ihre Sicherung sind an zwei verschiedenen Standorten in den Niederlanden redundant ausgelegt.

Das Infrastrukturmanagement konzentriert sich darauf, die verwalteten Server und die zugehörigen Infrastrukturkomponenten verfügbar und auf dem neuesten Stand zu halten. Zu diesem Zweck können die folgenden Aktivitäten definiert werden:

- Server-Verwaltung.
- Sicherheit.
- Überwachung.
- Back-up.

2.5.2 Regelmäßige Wartung

Unter regelmäßiger Wartung versteht man die Durchführung von korrigierenden, adaptiven oder präventiven Wartungsmaßnahmen. Dazu gehören regelmäßige Aktualisierungen der Umgebung und der Software (Firewall-Updates, Sicherheits-Patches, Betriebssystem usw.).

2.5.3 Anwendungsdienste

Die Anwendungsdienste kümmern sich um alle Aktivitäten im Zusammenhang mit der Bereitstellung von Anwendungen für Endnutzer. Die Anwendungsdienste betreffen die Bereitstellung von anwendungsorientierten Diensten für die Nutzer und umfassen die Planung, Ausführung und Kontrolle der täglichen Verwaltungsaufgaben. Sie gewährleistet auch den optimalen Betrieb einer oder mehrerer Anwendungen, so dass die gewünschte Funktionalität des Informationssystems für die Benutzer jederzeit verfügbar ist.

Sie umfasst die folgenden Dienstleistungen

- Überwachung: Überwachung der Anwendungsverfügbarkeit durch Überwachung von "Schlüsselereignissen der Anwendung".
- Patch Management: Anwendung von Patches, Updates und neuen Versionen von Anwendungssoftware.
- Daten sichern und wiederherstellen.
- Sicherheitsdienste.
- Verwaltung von Ressourcen auf der Anwendungsebene.

2.5.4 Dienstleistungen von Rechenzentren

Rechenzentrumsdienste bieten Betriebsmanagement, Wartung und Betrieb der gehosteten Serverkonfigurationen im Rechenzentrum, einschließlich der zugehörigen Betriebssysteme (OS), anderer Steuerungssoftwareprodukte und Peripheriegeräte. Die Dienste sind:

- Überwachung: Überwachung der Verfügbarkeit und Zuverlässigkeit der Serverkonfigurationen der im Rechenzentrum aufgestellten Server.
- Vorfallmanagement: Behandlung von Fehlern in der/den Serverkonfiguration(en) gemäß dem Vorfallmanagement Prozess.
- Vorbeugende Wartung zur Verhinderung von Zwischenfällen.
- Patch-Management: Anwendung von Patches und Updates auf Betriebssysteme und nicht anwendungsbezogene Softwareprodukte.
- Dokumentation.

2.5.5 Sicherungs- und Wiederherstellungsdienste

Sicherungs- und Wiederherstellungsdienste erstellen präventiv Kopien der vorhandenen Daten. Dadurch werden die Daten für den Fall gesichert, dass die Daten am ursprünglichen Speicherort verloren gehen oder beschädigt werden. Falls erforderlich, kann eine Sicherungskopie an ihrem ursprünglichen Speicherort wiederhergestellt werden. Die folgenden Aktivitäten werden durchgeführt:

- Überwachung: Überwachung, ob die Sicherung erfolgreich war oder nicht.
- Durchführung von Backups.
- Durchführung von Wiederherstellungen.
- Überwachung: Durchführung einer regelmäßigen Überwachung der Datensicherung.

RPO: Eine vollständige Sicherung wird wöchentlich durchgeführt. Eine Sicherung der SQL-Transaktionsprotokolle wird ebenfalls alle 30 Minuten durchgeführt. Dadurch wird der maximale Datenverlust bei erfolgreichen Backups auf 30 Minuten begrenzt. Die Backups werden einen Monat lang aufbewahrt.

Anträge wiederherstellen

Archive-IT wird einen Wiederherstellungsantrag innerhalb von 2 Arbeitsstunden nach Eingang des Antrags einleiten. Das RPO (Datum und Uhrzeit, bis zu dem die Wiederherstellung durchgeführt werden soll) der Wiederherstellungsanforderung sollte vom Kunden angegeben werden und kann bis zu einem

Monat zurückliegen. RTO (Vorlaufzeit einer Wiederherstellung) hängt von der Datenmenge ab. Während einer Wiederherstellung ist der Zugriff auf die virtuelle Archivumgebung nicht möglich.

Kontrollen zur Wiederherstellung und Backup

Mindestens einmal im Jahr finden im Hosting-Zentrum Tests zur Wiederherstellung der Datenbank statt, um den Wiederherstellungsprozess zu überprüfen. Falls erforderlich, werden Verbesserungsmaßnahmen ergriffen. Auch der Backup-Prozess wird überprüft und gegebenenfalls werden Abhilfemaßnahmen getroffen.

2.5.6 Sicherheitsdienste

Die Sicherheitspolitik ist in alle Archive-IT-Dienste eingebettet. Durch regelmäßige Audits wird überprüft, ob die Dienste in Übereinstimmung mit den Sicherheitsrichtlinien durchgeführt werden. Darüber hinaus sind die Sicherheitsrichtlinien und -verfahren für jeden Mitarbeiter von Archive-IT zugänglich.

Server und Speicher

Das von Archive-IT genutzte Rechenzentrum erfüllt die allgemeinen Anforderungen an die physische Sicherheit, wie Zugangskontrollen, Stromversorgung, Brandschutz usw. Die Infrastruktur wird 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr überwacht. Darüber hinaus gibt es verschiedene präventive Schutzmaßnahmen wie Firewall-Management, Standard-Virenschutz und Patch-Management.

Netzwerk

Das Netz ist die Grundlage für sichere Anwendungen und Informationsflüsse und damit für sichere Geschäftsprozesse. Vor allem die Integration von Sicherheitsmaßnahmen bietet Vorteile. Die Netzkomponenten müssen selbst für Sicherheit sorgen und intensiv mit den verschiedenen Sicherheitslösungen zusammenarbeiten, ohne dass die Infrastruktur zu starr wird.

Firewall-Dienste

Der Zweck einer Firewall in einem Computernetz bzw. auf einem Computer besteht darin, unerwünschten Datenverkehr aus einem Netzbereich an einem anderen zu hindern, um die Sicherheit in letzterem zu erhöhen. Bei dem geschützten Netz handelt es sich häufig um ein Intranet oder ein internes Netz, das vor dem Internet geschützt ist. Bei dem unerwünschten Datenverkehr handelt es sich beispielsweise um Angriffe von Hackern und Crackern (Knackern), Computerviren, Spyware und Denial-of-Service-Angriffe.

Die Firewall-Dienste ermöglichen die Einrichtung und das Betriebsmanagement einer Firewall, einschließlich einer dmz-Schnittstelle (demilitarisierte Zone).

Die folgenden Aktivitäten werden durchgeführt:

- Überwachung: Überwachung der Verfügbarkeit der Firewall-Konfigurationen.
- Firewall-Management: Sicherstellung des operativen Managements der Firewall-Konfigurationen einschließlich des zugehörigen Kontrollsystems.
- Vorbeugende Wartung zur Vermeidung von Zwischenfällen.

+ Dokumentation: Dokumentation der Firewall-Konfigurationen, der Systemsoftware und der Verfahren.

3. Exit- und Retransitionsplan

3.1 Umfang

Bei Beendigung des Vertragsverhältnisses kann es zu einer Übergabe der Daten von Archive-IT an den Kunden oder an Dritte kommen. Die Übermittlung von Daten beim Ausstieg und beim Übergang erfolgt auf der Grundlage der Ist-Situation der Verwaltung. Die bestehende Leistungserbringung wird während des Ausstiegs und des Übergangs auf der Grundlage der bestehenden Vereinbarungen in der Vereinbarung fortgesetzt.

Sind die Exit- und Retransition-Aktivitäten nach Vertragsende noch nicht abgeschlossen, werden diese Aktivitäten von Archive-IT - zu vereinbarten Kosten - bis zur endgültigen Entlassung durch den Kunden fortgeführt. Regelmäßige Änderungen an den bestehenden Diensten während des Ausstiegs und des Übergangs werden daher im Rahmen dieser Vereinbarungen erfolgen und fallen nicht in den Anwendungsbereich dieses Ausstiegs- und Übergangsplans.

Änderungen an der Infrastruktur, die sich aus der Übertragung ergeben, werden im Rahmen der zu diesem Zeitpunkt geltenden Standardänderungsverfahren vorgenommen. Erforderlichenfalls geht dem Beginn der Änderung eine inhaltliche Abstimmung zwischen den Fachleuten der Parteien voraus.

3.2 Kontinuität

Der Kunde wird so wenig wie möglich durch die Vertragsbeendigung, den Ausstieg und den Rückübergang belästigt. Die Parteien verpflichten sich, während des Ausstiegs- und Übergangsprozesses zusammenzuarbeiten. Archive-IT ist dafür verantwortlich, dass die vereinbarten Service Levels eingehalten werden..

3.3 Organisation

Für die Durchführung des Ausstiegs und des Übergangs ernennen die Parteien jeweils einen Ausstiegs- und Übergangsmanager. Die Ausstiegs- und Übergangsmanager sind die Ansprechpartner für jede Partei und verfügen über ein ausreichendes Mandat, um die in diesem Ausstiegs- und Übergangsplan vereinbarten Vereinbarungen zu erfüllen. Hinsichtlich des Umfangs des Mandats sollten interne Mandatierung, Governance-Regeln und Einschränkungen berücksichtigt werden. Die Umsetzung dieses Ausstiegs- und Umstellungsplans wird zügig in Angriff genommen werden. Die Parteien werden ihre Zeitpläne nach besten Kräften koordinieren, um den Ausstieg und den Übergang so schnell wie möglich zu gestalten. Archive-IT stellt ausreichend und gut qualifiziertes Personal und andere Ressourcen für die Durchführung eines kontrollierten Ausstiegs und Rückübergangs zur Verfügung.

3.4 Akzeptanz, Entlastung

Die Entlastung erfolgt mit der Annahme der Übertragung der betreffenden Dienstleistungen durch den Kunden. Bei der Entlassung können Restbestände vorhanden sein. Nach der Entlassung prüfen die Parteien, welche Restposten noch offen sind und erledigt werden müssen.

3.5 Aktivitäten und Ergebnisse

Die von Archive-IT im Rahmen des Exits und der Retransition erbrachten Leistungen müssen von Archive-IT geliefert werden, ebenso wie die Deliverables. In jedem Fall muss ein sicherer und transparenter Datenexport auf einem Datenträger erfolgen, der für den Kunden zu diesem Zeitpunkt lesbar und sicher ist.

Archive-IT wirkt bei der Beantwortung von Fragen mit, die innerhalb der vereinbarten Fristen gestellt werden (Fragen des Auftraggebers und/oder der an der Übertragung beteiligten Dritten). Findet der Auftraggeber die Fristen nicht angemessen und stört er sich daran, müssen die Parteien eine neue Frist vereinbaren. Die Bestimmungen von Archive-IT zur Daten- und Informationssicherheit bleiben bis zur Übergabe der Daten und sonstigen Informationen erhalten. Archive-IT wird seine Verpflichtungen im Rahmen dieses Ausstiegs- und Rückübertragungsplans nicht aussetzen, wenn ein Konflikt über die Beendigung der Zusammenarbeit auftritt.

3.6 Liefergegenstände Archive-IT

Die folgenden Leistungen sind zu erbringen:

- Analyse der Ausfuhren und Abstimmung mit dem Kunden.
- Aufzeichnen oder bestimmen:
  - in welchem Format die Daten und Metadaten bereitgestellt werden sollen.
  - Ob die Historie der Dateien einbezogen werden soll.
  - Ob Versionen der digitalen Dokumente aufgenommen werden sollen.
- Die Klärung weiterer Fragen, wie zum Beispiel:
  - Wie viele Exportläufe wir durchführen sollten (Testläufe und Produktionslauf).
  - Wie oft sollten wir die Daten liefern und wie?

Archive-IT wird innerhalb von vier Wochen nach dem Ausreiseantrag eine Analyse erstellen und ausarbeiten. Archive-IT wird nach der Beauftragung innerhalb von zwei Wochen mit der Erstellung des Exportdienstes beginnen.

3.7 Vertrauliche Informationen

Die Parteien respektieren die Interessen der anderen Seite, das geistige Eigentum und die Vertraulichkeit von Informationen. Die Verschwiegenheitspflicht von Archive-IT besteht auch nach dem Ausscheiden und der Rückübereignung unbefristet fort.

3.8 Ausstiegs-/Übergangskosten

Archive-IT stellt sicher, dass bei Beendigung der Vereinbarung die Exit- und Retransition-Aktivitäten und -Leistungen wie in diesem Dokument beschrieben durchgeführt oder geliefert werden. Die Kosten im Zusammenhang mit dem Exit und der Retransition der digitalen/physischen Daten gehen zu Lasten des Auftraggebers. Vor der Durchführung eines Ausstiegs- oder Übergangsprojekts wird Archive-IT ein Angebot unterbreiten.

4. KPIs-Software SaaS-Software

Nr.	KPI	Beschreibung	Standard	Anmerkungen
1	Verfügbarkeit	Verfügbarkeit der SaaS-Umgebung	99,9%	Gemessen innerhalb des Servicefensters 24/7, ohne geplante Wartung.
2	Sicherheits-management	Antiviren-Software auf dem neuesten Stand halten	100% < 36 Stunden nach Veröffentlichung der Updates	Wenn ein Viren-/Antispam-Update für den Virenscanner herauskommt, wird es auf die entsprechenden Systeme ausgerollt.
3	Sicherheits-management	Implementierung von kritischen Sicherheitsupdates	100% < 72 Stunden	Archive-IT stellt sicher, dass die neuesten Sicherheitsupdates installiert sind.
4	Backup	Sicherung und Wiederherstellung durchführen	Kontinuierlich alle 30 Minuten	Tägliche Sicherung der in der gehosteten Umgebung gespeicherten Kundendaten.
5	Wiederherstellen	Maximaler Datenverlust	30 Minuten	Die maximale Zeitspanne, in der hinzugefügte oder geänderte Daten verloren gehen können. Gilt für alle Produktionsdaten.
6	Performance Virtual Archive	Ein Bild ist innerhalb von fünf Sekunden verfügbar	90 % der abgerufenen Bilder sind innerhalb der Fünf-Sekunden-Frist verfügbar.	Die Definition besagt, dass die Übersicht über die gescannten Dateien innerhalb von fünf Sekunden auf dem Bildschirm erscheint. Das anschließende Anklicken einer bestimmten Datei erfolgt ebenfalls innerhalb von fünf Sekunden. Dabei wird von einer optimal verfügbaren Internet-Bandbreite ausgegangen.