Service Level Agreement

Archive-IT - SaaS

Date	**03-09-2025**
Version	**1.5**

secure yesterday,
empower tomorrow.

Table des matières

1.1 Introduction 4

1.2 Termes et définitions 4

2.1 Soumission des incidents/notifications 6

2.1.1 Disponibilité du support 6

2.1.2 Incident management 6

2.1.3 Délais de réponse et de résolution 7

2.1.4 Rapports sur les Incidents/Notifications 8

2.2 Maintenance planifiée 8

2.3 Change- et Release Management 9

2.4 Escrow logiciel 9

2.5 Paramètres de service SaaS 9

2.5.1 Disponibilité 9

2.5.2 Maintenance régulière 10

2.5.3 Services applicatifs (Application Services) 10

2.5.4 Datacenter services 10

2.5.5 Services de sauvegarde et de restauration 11

2.5.6 Services de sécurité 11

3.1 Champ d'application 13

3.2 Continuité 13

3.3 Organisation 13

3.4 Acceptation, décharge 14

3.5 Activités et livrables 14

3.6 Livrables Archive-IT 14

3.7 Informations confidentielles 15

3.8 Coûts de l'exit/de la transition 15

Historique des versions

Auteur	Version	Date	Modification(s)
Roy Peeters	Concept	02-07-2018	
Hein Boots	1.0	09-05-2019	Compléments suite à discussions mutuelles
Roy Peeters	1.1	26-03-2021	Ajustements des livrables
Roy Peeters	1.2	30-11-2021	Petites modifications textuelles
Roy Peeters	1.3	04-03-2022	Horaires d'ouverture ajustés
Hein Boots	1.4	18-7-2024	Mise à jour de divers points
Marketing	1.5	03-09-2025	Nouvelle présentation / mise en page

1. Généralités

1.1 Introduction

Dans cette Service Level Agreement (SLA), les niveaux de service d'Archive-IT concernant le logiciel SaaS sont détaillés et expliqués.

1.2 Termes et définitions

Les termes écrits avec une majuscule dans cette SLA ont la signification indiquée dans la liste de définitions ci-dessous, ou, si le terme n'y figure pas, la signification qui lui est attribuée dans l'une des autres parties du Contrat :

Terme	Définition
Département Support	Le département Support de Archive-IT
Gestion	La gestion proactive, réactive et adaptative du service SaaS visant sa disponibilité et sa continuité. Cela inclut la mise en œuvre de correctifs, de nouvelles versions et de nouvelles releases des applications et logiciels systèmes sous-jacents.
Disponibilité	La norme de disponibilité du service SaaS est exprimée en pourcentage du temps durant lequel, pendant la Fenêtre de Service, le service SaaS peut être utilisé. Formule : [(Fenêtre de Service– Temps d'Indisponibilité)/ (Fenêtre de Service)] X 100% La disponibilité désigne la capacité technique de se connecter au portail de Archive-IT donnant accès au service SaaS et de fournir les fonctionnalités convenues
Changement	Une modification/ajustement d'une partie du service SaaS.
Change Advisory Board (CAB)	Les personnes responsables de l'approbation des demandes de changement (RFC).
Change Manager	Responsable final du Change Advisory Board.
Temps d'indisponibilité	Période durant laquelle le service SaaS n'est pas disponible dans la Fenêtre de Service.
Incident	Événement opérationnel qui ne fait pas partie du fonctionnement standard du service SaaS et entraînant une dégradation du service opérationnel convenu

Notification	Questions générales, demandes ou plaintes qui ne constituent pas un Incident.
Maintenance	Exécution de travaux de maintenance corrective, adaptative ou préventive. Cela inclut les mises à jour régulières de l'environnement et des logiciels (mises à jour de pare-feu, correctifs de sécurité, système d'exploitation, etc.).
Fenêtre de maintenance	Période pendant laquelle Archive-IT (a) effectue des travaux de maintenance planifiés et (b) réalise des maintenances supplémentaires nécessaires qui ne peuvent être reportées (par exemple pour des risques de sécurité).
Temps de résolution	Nombre d'heures ouvrables entre le moment où un Incident est pris en charge et le moment où il est résolu.
Correctif ou Patch	Modification des applications ou logiciels systèmes sous-jacents pour corriger des erreurs.
Problème	Situation indésirable identifiée à partir d'Incidents connexes, dont la cause n'est pas encore connue.
Temps de réponse	Temps écoulé entre la notification de l'Incident par le Client selon la procédure convenue et le moment où Archive-IT prend en charge la notification.
RFC – Request for Change	Une RFC est synonyme de Ticket de Changement. Demande de modification d'une partie du service SaaS.
Fenêtre de Service	Période pendant laquelle le service SaaS est fourni, déduction faite de la Fenêtre de maintenance.
Jours ouvrables	Du lundi au vendredi, à l'exception des jours fériés nationaux (néerlandais) reconnus (comme indiqué sur le site du gouvernement).
Heures ouvrables	De 08h15 à 17h00 les jours ouvrables.
Solution de contournement (Workaround)	Solution temporaire pour un Incident.

2. Logiciel

2.1 Soumission des incidents/notifications

Pour les Incidents/Notifications concernant le logiciel de Archive-IT, vous devez vous adresser au département Support via le portail de support en ligne sécurisé. Les Incidents/Notifications peuvent être enregistrés 24h/24 et 7j/7. Vous pouvez également consulter dans ce portail la progression et l'historique de vos Incidents/Notifications.

Si vous n'y avez pas encore accès, vous pouvez en faire la demande à l'adresse support@archive-it.group.

2.1.1 Disponibilité du support

Le département Support assure le suivi et la communication sur l'état des Incidents/Notifications. Le département Support est disponible les jours ouvrables de 08h15 à 17h00. Il n'y a pas de permanence les week-ends et jours fériés.

En cas d'urgence élevée, un Incident peut également être signalé ou expliqué par téléphone (jours ouvrables / heures ouvrables). Le département Support est joignable au numéro de téléphone +31 77 750 11 00.

Archive-IT met tout en œuvre pour résoudre les Incidents dans les délais de résolution définis (voir chapitre sur les délais de réponse et de résolution).

2.1.2 Incident management

Les étapes suivantes sont suivies après la réception d'un Incident/Notification :

- Classification et priorisation.
- Suivi de la progression jusqu'à la clôture definitive.
- Communication des informations sur le statut.
- Traitement des Incidents/Notifications.

Un Incident peut donner lieu à une Request For Change (RFC).
Les Incidents/Notifications peuvent conduire à une RFC. L'Incident/la Notification sera alors temporairement mis en attente, avec référence à la RFC. En cas d'urgence élevée, il peut être décidé de proposer une solution temporaire (Workaround) ou de mettre en œuvre un correctif (Fix) dans le délai de résolution défini.

Durée de conservation des pièces jointes et captures d'écran
Les pièces jointes et captures d'écran des tickets de support sont conservées pendant un an.

Pendant cette période, ces fichiers peuvent être consultés, même dans les tickets fermés. Lorsque le ticket est fermé depuis plus d'un an, toutes les pièces jointes et captures d'écran sont supprimées et ne sont plus accessibles. Cela permet d'éviter la conservation inutile d'informations sensibles.

2.1.3 Délais de réponse et de résolution

Les délais de réponse et de résolution sont définis en fonction de l'impact déclaré et de la classification. La combinaison de ces deux éléments détermine la priorité.

Détermination du code d'impact

Code d'impact	Étendue de l'Incident
Élevé	Plus de 10 utilisateurs ou processus critiques de l'entreprise
Moyen	2 à 10 utilisateurs
Faible	1 utilisateur

Détermination de la classification de l'incident

Code d'impact	Étendue de l'Incident
Élevé	Travail impossible ou affecte des processus critiques de l'entreprise
Moyen	Travail difficile
Faible	Travail possible

Détermination de la priorité

La combinaison du **code d'impact** et de **la classification** détermine la priorité d'un Incident.

Priorité Classification			
Code d'impact	**Élevé** **(travail impossible)**	**Moyen** **(travail difficile)**	**Faible** **(travail possible)**
Élevé (> 10 utilisateurs)	I	I	II
Moyen (2-10 utilisateurs)	I	II	III
Faible (1 utilisateur)	III	III	III

Détermination de l'urgence

Selon la priorité, l'urgence sera déterminée conformément à la matrice ci-dessus.

Délais de réponse et de résolution		
Priorité	**Délai de réponse**	**Délai de résolution**

I (urgent)	< 1 jour ouvrable	< 1 jour ouvrable
II (moins urgent)	< 1 jour ouvrable	< 1 semaine ouvrable
III (non urgent)	< 1 jour ouvrable	< 1 mois

Archive-IT s'efforcera également de résoudre les Incidents dont la cause n'est pas imputable à Archive-IT. Cependant, Archive-IT n'applique pas de « délais de résolution » pour ces Incidents. Archive-IT est en droit de demander une rémunération pour les travaux effectués dans ce cadre, selon ses tarifs habituels en vigueur à ce moment-là.

2.1.4 Rapports sur les Incidents/Notifications

Via le portail de support en ligne, vous pouvez générer les rapports suivants :

- Le nombre d'Incidents.
- Pour chaque Incident, le « Délai de résolution » et le « Délai de réponse ».
- Le nombre d'Incidents regroupés par priorité.
- Une liste des Incidents et RFC ouverts.

2.2 Maintenance planifiée

La maintenance planifiée du service SaaS a lieu en dehors des heures et jours ouvrables, pendant la Fenêtre de maintenance.

Maintenance au niveau du système d'exploitation et de l'infrastructure
Cela concerne les mises à jour (de sécurité) au niveau du système d'exploitation (mises à jour Windows) et, le cas échéant, la maintenance de l'infrastructure, effectuée par notre partenaire d'hébergement. Cette maintenance est testée de manière approfondie par Archive-IT dans l'environnement d'acceptation une semaine avant sa mise en production. En cas de problèmes constatés (ou prévisibles), le déploiement dans les environnements de production d'Archive-IT sera reporté.

En règle générale, cette maintenance a lieu le mercredi soir/nuit entre 20h00 et 01h00. Environ 13 interventions de maintenance sont prévues par an et sont annoncées à l'avance, mais au moins 4 jours ouvrables avant la date prévue.

Maintenance du logiciel Archive-IT
Lors de la maintenance régulière du logiciel Archive-IT, la disponibilité n'est pas compromise (sauf dans des cas exceptionnels, qui seront immédiatement communiqués par Archive-IT), car l'architecture SaaS d'Archive-IT et le mécanisme de déploiement global permettent un déploiement sans impact sur la disponibilité. En cas de problème, il est possible de revenir facilement et rapidement à une version précédente.

Cette maintenance a lieu – selon les besoins ou nécessités – en dehors des heures ouvrables et est annoncée à l'avance, au minimum 4 jours ouvrables avant l'intervention.

2.3 Change- et Release Management

Les demandes de modification du logiciel doivent également être soumises via le portail de support en ligne. Archive-IT évalue la faisabilité et les conséquences de la modification proposée (y compris les coûts) et détermine si, et dans quelle mesure, la modification sera mise en œuvre. Une demande de modification qui n'est pas approuvée sera rejetée par Archive-IT, avec justification.

Pour les mises à jour importantes, des **Release Notes** sont établies.

2.4 Escrow logiciel

Les parties attachent de l'importance à la continuité, tant pour le logiciel que pour les données hébergées. Vous pouvez compter sur Archive-IT à cet égard. Si vous souhaitez une sécurité supplémentaire, Archive-IT a identifié un partenaire fiable capable de fournir un dispositif d'Escrow solide. Pour toute demande d'information ou mise en place d'Escrow, veuillez contacter Archive-IT.

2.5 Paramètres de service SaaS

2.5.1 Disponibilité

Le service SaaS est fourni sur une plateforme de type Infrastructure-as-a-Service avec une **garantie de disponibilité*** de 99,9 %. Ceci se fait en collaboration avec le partenaire de datacenter, depuis des datacenters situés aux Pays-Bas.

* Dans ce contexte, « non disponible » signifie : indisponibilité totale pour tous les utilisateurs.

L'infrastructure sous-jacente répond à des exigences strictes en matière de sécurité, garantit une haute disponibilité et une exécution redondante de toutes les ressources primaires. Toutes les données et leurs sauvegardes sont stockées de manière redondante sur deux sites distincts aux Pays-Bas.

La gestion de l'infrastructure vise à maintenir les serveurs gérés et les composants d'infrastructure associés disponibles et à jour. Les tâches suivantes peuvent être définies à cet effet :

- Gestion des serveurs (Server Management)
- Sécurité

- Supervision/Monitoring
- Sauvegarde (Back-up)

2.5.2 Maintenance régulière

Par maintenance régulière, on entend l'exécution de travaux de maintenance corrective, adaptative ou préventive. Cela inclut les mises à jour régulières de l'environnement et des logiciels (mises à jour de pare-feu, correctifs de sécurité, système d'exploitation, etc.).

2.5.3 Services applicatifs (Application Services)

Les services applicatifs couvrent toutes les activités liées à la fourniture d'applications aux utilisateurs finaux. Les services applicatifs concernent la fourniture de services orientés applications aux utilisateurs et comprennent la planification, l'exécution et le contrôle des tâches de gestion quotidienne. Ils assurent également le fonctionnement optimal d'une ou plusieurs applications, de manière à ce que les fonctionnalités souhaitées du système d'information soient disponibles pour les utilisateurs à tout moment.

Ces services comprennent :

- Surveillance (Monitoring) : suivi de la disponibilité des applications en surveillant les « événements clés de l'application ».
- Gestion des correctifs (Patch Management) : application de correctifs, mises à jour et nouvelles versions des logiciels applicatifs.
- Sauvegarde et restauration des données (Back-up & Restore).
- Services de sécurité (Security Services).
- Gestion des ressources au niveau applicatif (Application-level Resource Management).

2.5.4 Datacenter services

Les services de datacenter assurent la gestion opérationnelle, la maintenance et l'exploitation des configurations serveur hébergées dans le datacenter, y compris les systèmes d'exploitation (OS), autres logiciels de gestion et périphériques associés. Les services comprennent :

- Surveillance (Monitoring) : suivi de la disponibilité et de la fiabilité des configurations serveur hébergées dans le datacenter.
- Gestion des incidents (Incident Management) : traitement des pannes affectant les configurations serveur conformément au processus de gestion des incidents.
- Maintenance préventive pour prévenir les incidents.
- Gestion des correctifs (Patch Management) : application de correctifs et mises à jour sur les OS et logiciels non liés aux applications.

+ Documentation.

2.5.5 Services de sauvegarde et de restauration

Les services de sauvegarde et de restauration permettent de créer de manière préventive des copies des données existantes. Ainsi, ces données sont protégées en cas de perte ou de corruption des données à leur emplacement d'origine. Si nécessaire, une sauvegarde peut être restaurée à son emplacement initial. Les activités suivantes sont réalisées :

+ Surveillance (Monitoring) : contrôle de la réussite ou de l'échec des sauvegardes.
+ Réalisation des sauvegardes (Back-up).
+ Restauration des données (Restore).
+ Contrôle : réalisation de contrôles périodiques des sauvegardes.

RPO (Recovery Point Objective) : Une sauvegarde complète est effectuée chaque semaine. De plus, une sauvegarde des journaux de transactions SQL est réalisée toutes les 30 minutes. La perte maximale de données en cas de sauvegardes réussies est ainsi limitée à 30 minutes. Les sauvegardes sont conservées pendant un mois.

Demandes de restauration

Archive-IT ancera une demande de restauration dans les 2 heures ouvrables suivant sa réception. La RPO (date et heure auxquelles les données doivent être restaurées) doit être indiquée par le Client et peut remonter au maximum à un mois. Le RTO (Recovery Time Objective) dépend de la quantité de données. Pendant la restauration, l'environnement de Virtual Archive n'est pas accessible.

Mesures de contrôle des sauvegardes et restaurations

Au moins une fois par an, un test de restauration de base de données est réalisé dans le centre d'hébergement pour contrôler le processus de restauration. Des actions correctives sont entreprises si nécessaire. Le processus de sauvegarde est également contrôlé et, si nécessaire, des mesures correctives sont appliquées.

2.5.6 Services de sécurité

La politique de sécurité est intégrée dans tous les services de Archive-IT. Des audits réguliers sont effectués pour vérifier que les services sont fournis conformément aux directives de sécurité. De plus, les directives et procédures de sécurité sont accessibles à chaque collaborateur de Archive-IT.

Serveurs et stockage

Le datacenter utilisé par Archive-IT respecte les exigences générales en matière de sécurité physique, telles que le contrôle d'accès, l'alimentation électrique, la protection contre

l'incendie, etc. L'infrastructure est surveillée 24h/24, 7j/7, 365 jours par an. Diverses mesures de protection préventives sont également mises en place, telles que la gestion des pare-feu, l'antivirus standard et la gestion des correctifs.

Réseau

Le réseau constitue la base pour des applications et flux d'information sécurisés, et donc pour des processus d'entreprise sûrs. L'intégration des mesures de sécurité apporte des avantages. Les composants du réseau doivent offrir eux-mêmes une sécurité et collaborer étroitement avec les différentes solutions de sécurité, sans rendre l'infrastructure trop rigide.

Services de pare-feu

Un pare-feu a pour objectif, dans un réseau informatique ou sur un ordinateur, d'empêcher que du trafic indésirable d'une zone réseau ne parvienne à une autre, afin d'améliorer la sécurité de cette dernière. Le réseau protégé est généralement un intranet ou réseau interne, et il est protégé contre Internet. Le trafic indésirable comprend, par exemple, des attaques de hackers et crackers, virus informatiques, logiciels espions et attaques par déni de service (DoS).

Les services de pare-feu assurent la configuration et la gestion opérationnelle d'un pare feu, y compris une interface DMZ (zone démilitarisée).

Les activités suivantes sont réalisées :

- Surveillance (Monitoring) : suivi de la disponibilité des configurations du pare-feu.
- Gestion du pare-feu (Firewall Management) : gestion opérationnelle des configurations du pare-feu, y compris le système de contrôle associé.
- Maintenance préventive pour prévenir les incidents.
- Documentation : documentation des configurations du pare-feu, des logiciels système et des procédures.

3. Exit- en retransitieplan

3.1 Champ d'application

À la fin du contrat, un transfert des données peut être effectué d'Archive-IT vers le client ou un tiers. Le transfert des données durant l'exit et la retransition se fait sur la base de l'état de gestion « tel quel (as-is) ». Le service existant continue pendant l'exit et la retransition conformément aux accords existants du contrat.

Si les travaux d'exit et de retransition ne sont pas terminés à la fin du contrat, ces travaux seront poursuivis par Archive-IT – aux coûts convenus – jusqu'à la décharge finale par le client. Les modifications régulières du service existant durant l'exit et la retransition interviennent donc dans le cadre de ces accords et ne relèvent pas du périmètre de ce plan d'exit et de retransition.

Les modifications d'infrastructure résultant du transfert sont réalisées selon les procédures standard de changement en vigueur à ce moment. Si nécessaire, le démarrage du changement est précédé d'une coordination technique entre les spécialistes des deux parties.

3.2 Continuité

Le client subira le moins de perturbations possible du fait de la résiliation du contrat et du processus d'exit et de retransition. Les parties s'engagent à collaborer pendant l'ensemble du processus d'exit et de retransition. Archive-IT est responsable du maintien des niveaux de service convenus.

3.3 Organisation

Pour l'exécution de l'exit et de la retransition, chaque partie désigne un manager exit et retransition. Les managers exit et retransition constituent le point de contact pour chaque partie et disposent d'un mandat suffisant pour respecter les engagements prévus dans ce plan. La portée du mandat doit tenir compte des règles internes de délégation et de gouvernance, ainsi que de leurs limites.

L'exécution de ce plan d'exit et de retransition sera menée avec diligence. Les parties coordonneront leurs plannings dans la mesure du possible afin d'assurer une exit et retransition rapides. Archive-IT met à disposition un personnel suffisant et qualifié, ainsi que les autres ressources nécessaires pour garantir une exit et retransition contrôlées.

3.4 Acceptation, décharge

La décharge a lieu lors de l'acceptation par le Client du transfert du service concerné. Lors de la décharge, il peut subsister des points en suspens. Après la décharge, les Parties examineront quels points restent ouverts et doivent être traités.

3.5 Activités et livrables

Les activités réalisées par Archive-IT dans le cadre de l'exit et de la retransition doivent être livrées par Archive-IT, ainsi que les livrables correspondants. En tout état de cause, une exportation de données sécurisée et transparente doit être effectuée sur un support de données sécurisé, lisible par le Client et conforme aux standards en vigueur à ce moment-là.

Archive-IT collaborera à la fourniture de réponses aux questions posées dans les délais convenus (questions du Client et/ou de tiers impliqués dans le transfert). Si le Client estime que les délais ne sont pas raisonnables et en subit les conséquences, un nouveau délai devra être convenu entre les Parties. Les dispositions de Archive-IT en matière de sécurité des données et de l'information restent en vigueur jusqu'au transfert des données et de toute autre information éventuelle. Archive-IT ne suspendra pas ses obligations issues du présent plan d'exit et de retransition en cas de conflit relatif à la fin de la collaboration.

3.6 Livrables Archive-IT

Les livrables suivants s'appliquent :

- Réaliser une analyse de l'exportation et la coordonner avec le Client.
- Définir ou déterminer :
  - Dans quel format les données et les métadonnées doivent être fournies.
  - Si l'historique des dossiers doit être inclus.
  - Si les versions des documents numériques doivent être incluses.
- Examiner d'autres questions telles que :
  - Combien de runs d'exportation doivent être effectués (tests et production).
  - À quelle fréquence et de quelle manière les données doivent être fournies.

Archive-IT finalisera et développera l'analyse dans les quatre semaines suivant la demande d'exit.
Archive-IT commencera la mise en place du service d'exportation dans les deux semaines suivant la commande.

3.7 Informations confidentielles

Les Parties respectent les intérêts, la propriété intellectuelle et la confidentialité des informations de chacun.
L'obligation de confidentialité d'Archive-IT demeure en vigueur après l'exit et la retransition pour une durée indéterminée.

3.8 Coûts de l'exit/de la transition

Archive-IT veille à réaliser et livrer les activités et les livrables liés à l'exit et à la retransition à la fin du contrat, tels que décrits dans le présent document. Les coûts liés à l'exit et à la retransition concernant les données numériques et/ou physiques sont à la charge du Client. Avant de réaliser un projet d'exit ou de transition, Archive-IT soumettra un devis.

4. KPI's logiciel SaaS

Nr.	KPI	Description	Norme	Explications
1	Disponibilité	Disponibilité de l'environnement SaaS	99,9%	Mesurée dans la fenêtre de service 24/7, à l'exception de la maintenance planifiée.
2	Gestion de la sécurité	Maintien à jour du logiciel antivirus	100% < 36 heures après la sortie des mises à jour	Dès qu'une mise à jour antivirus/antispam est publiée, elle est déployée sur les systèmes concernés.
3	Gestion de la sécurité	Application des mises à jour de sécurité critiques	100% < 72 heures	Archive-IT veille à disposer des dernières mises à jour de sécurité.
4	Sauvegarde	Exécution des sauvegardes et restauration	Continue toutes les 30 minutes	Sauvegarde quotidienne des données du Client stockées dans l'environnement hébergé.
5	Restauration	Perte de données maximale	30 minutes	Durée maximale pendant laquelle les données ajoutées ou modifiées peuvent être perdues. S'applique à toutes les données de production.
6	Performance Virtual Archive	Une image est disponible en moins de cinq secondes	90% des images demandées sont disponibles dans le délai de cinq secondes	La définition est que l'aperçu des dossiers scannés s'affiche à l'écran en moins de cinq secondes. L'accès à un dossier spécifique doit également se faire en moins de cinq secondes. Cela suppose une bande passante Internet optimale.