

Objet	L'objet de ce document est de décrire de façon spécifique et détaillée les enjeux, le périmètre de la politique d'archivage contractuelle entre le client et be ys trusted solutions france afin d'utiliser notre SAE ArchiveMi ainsi que la gouvernance des archives pour le compte du Client.
-------	---

Version	Date	Modifications	Rédacteur
0.1	27/06/2017	Création du document	GD BIONNIER
0.2	16/01/2018	Mise à jour et complétion de certains paragraphes	GD BIONNIER
0.3	15/02/2018	Remplissage du taux de disponibilité	B CROIZET
0.4	07/03/2018	Complétion des paragraphes manquants, corrections, approbations et mise à jour des schémas	B CROIZET
1.0	12/07/2018	Mise à jour et complétion de certains paragraphes	GD BIONNIER
1.1	02/11/2018	Relecture	S PASSELERGUE
2.0	09/01/2019	Prise en compte des remarques	GD BIONNIER
2.1	3/03/2020	Suppression du terme « mettre logo du client » sur l'entête	GD BIONNIER
2.2	1/12/2020	Adaptation pour un client	S PASSELERGUE
3.0	20/12/2021	Changement de structure : passage du DDTS au DGTS de la nouvelle norme NF Z42-013 d'octobre 2020	GD BIONNIER
3.1	27/06/2022	Ajout d'un paragraphe sur la gestion de l'élimination des archives	GD BIONNIER
3.2	01/07/2022	Audit interne documentaire	MNGR
3.3	27/09/2022	Ajout de la fonctionnalité de gel / dégel des archives et de l'exhaustivité des archives pour assurer aucune perte de données	GD BIONNIER
3.4	24/01/2022	Ajout de l'organisation des documents d'archives	GD

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

	3	dans le SIP Transfert de responsabilité entre le Client et le Prestataire Complément sur le contrôle des formats	BIONNIER
3.5	20/04/2023	Complément sur la présence ou non d'une politique d'archivage d'un client + Distinction entre la procédure de restitution et celle de réversibilité + Compléments d'informations dans la procédure d'élimination en ajoutant le fait que le client puisse procéder à cette gestion + Ajout d'une phrase au niveau des formats acceptés en précisant que la liste n'est pas exhaustive et que le contrôle mis en place s'adapte selon les formats à archiver	GD BIONNIER
3.6	09/05/2023	Mise à jour du glossaire « Service versant », « Service producteur », « Service d'archive » + Exemple en cas de conversion de format + Mise à jour du chapitre sur la réversibilité	GD BIONNIER
3.7	30/06/2023	Mise en place d'un OID sur la politique d'archivage	GD BIONNIER
3.8	14/02/2024	Revue annuelle avec changement de la direction	GD BIONNIER
3.9	02/01/2025	Changement de la direction + Changement coordonnées du site de backup	GD BIONNIER
4.0	30/10/2025	Changement de siège social, de dénomination de la solution ID-Archive par ArchiveMi et changement de l'OID	GD BIONNIER
4.1	19/02/2026	Ajout section sur la prise en compte du cadre normatif et réglementation sectoriel + Ajout d'un paragraphe sur la veille opérée + Ajout explications du numéro OID + Restructuration des paragraphes sans apporter de modification	GD BIONNIER

* <Version>.<Edition> Changement de version = évolution majeure Changement d'édition = évolution mineure

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Durée de validité	Nombre de versions à conserver
1 an	Minimum 2 (actuelle + précédente)

Niveau de diffusion	Liste de diffusion si Restreint ou Confidentiel
Public	Interne be ys trusted solutions France (BYTSF) et clients BYTSF

	Fonction	Date & Signature
Vérificateur 1	<i>Administrateur SAE / backup</i>	
Approbateur	<i>Directeur Général</i>	

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Sommaire

1	Présentation générale.....	10
1.1	Enjeux liés à l'archivage électronique.....	10
1.2	Cadre normatif et réglementaire appliqué.....	11
1.3	Cadre normatif et réglementation sectoriel applicables.....	11
1.4	Niveau de sécurité physique et informatique respecté.....	12
1.5	Gestion de la politique ArchiveMi	12
1.5.1	Identification du document.....	12
1.5.2	Circonstances dans lesquelles l'OID doit être modifié.....	12
2	Objectifs d'un système d'archivage électronique.....	13
3	Parties prenantes, rôles et responsabilités.....	14
3.1	Le Client.....	14
3.2	Les utilisateurs client.....	14
3.3	be ys trusted solutions France.....	14
4	Différence entre archives privées et archives publiques.....	16
4.1	Cycle de vie des documents d'archives privées.....	16
4.2	Cycle de vie des documents d'archives publiques.....	17
4.3	Gestion du cycle de vie.....	18
5	Composition des SIP (paquets en entrée).....	19
5.1	Organisation des documents d'archives dans le SIP.....	19
5.2	Organisation des métadonnées dans le SIP.....	19
5.3	Transfert entre le Service Versant et le Service d'Archivage.....	20
5.4	Gestion des métadonnées.....	21
5.5	Indexation des documents.....	22
5.6	Formats d'archivage.....	22
5.6.1	Liste des formats autorisés.....	22
5.6.2	Mécanisme de contrôle du format.....	23
5.7	Conversion dans un format plus pérenne.....	23
5.8	Veille technologique et lutte contre l'obsolescence des formats.....	24
5.9	Intégrité des archives.....	25
6	Gestion du cycle de vie.....	26
6.1	Application du sort final.....	26

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.1.1	Cas des archives privées.....	26
6.1.2	Cas des archives publiques.....	26
6.2	Gestion de l'élimination des archives.....	26
6.2.1	Traitement des archives à éliminer par le Client.....	27
6.2.2	Délégation des archives à éliminer au Prestataire.....	28
6.2.3	Finalisation du traitement.....	29
6.3	Gestion de la restitution des archives.....	30
6.3.1	Mode opératoire.....	30
7	Gel / Dégel des archives.....	31
7.1	Introduction.....	31
7.2	Geler une archive.....	31
7.3	Dégeler une archive.....	32
8	Traçabilité.....	33
9	Exhaustivité des documents.....	34
10	Sécurisation de l'information.....	35
10.1	Introduction et présentation de nos datacenters.....	35
10.2	Sécurité physique, bâtementaire et électronique.....	37
10.2.1	La sécurité physique de notre infrastructure.....	38
10.3	La sécurité de notre Système d'Information.....	40
10.4	Antivirus centralisé et patch de sécurité.....	40
10.5	Intrusions.....	41
10.6	Sécurisation des échanges.....	41
10.7	Protection des données personnelles.....	41
10.8	Conformité règlementaire et juridique.....	41
10.9	Réplication des archives.....	42
10.10	Horodatage.....	42
10.11	Continuité de service.....	42
11	Principes techniques de la réversibilité.....	44
11.1	Principe.....	44
11.2	Mode opératoire.....	44
12	Fonctionnement du service.....	46
12.1	Auditabilité.....	46
12.2	Niveau de service.....	46

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés **be ys trusted solutions France** - Toute reproduction ou diffusion même partielle interdite sans autorisation

Glossaire / Abréviations

Terme	Définition
Acteurs / Rôles	Personnes ou profils chargés d'une activité particulière dans le projet d'archivage. On distingue cinq profils : le management, la coordination (du projet puis du système d'archivage), l'expertise juridique ou métier des documents, la gestion technique du stockage et de la conservation, et les utilisateurs qui produisent ou utilisent les documents archivés.
Archives	Ensemble de documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité.
Archivage	Démarche d'organisation qui a pour objectif d'identifier, de mettre en sécurité et de maintenir disponibles l'ensemble des documents qui engagent une entreprise ou un organisme vis-à-vis de tiers ou de son activité future et dont le défaut représenterait un risque.
Authenticité	Caractère d'un document dont on peut prouver qu'il est bien ce qu'il prétend être, qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu, et qu'il a été produit ou reçu au moment où il prétend l'avoir été.
Authentification unique	L'authentification unique (en anglais Single Sign-On : SSO) est une méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.
Bordereau de versement	Pièce justificative de l'opération de versement comportant le relevé détaillé des documents ou dossiers remis à un service d'archives par un service versant : le bordereau de versement tient lieu de procès-verbal de prise en charge et d'instrument de recherche.
Bordereau d'élimination	Etat des documents soumis par un service producteur au visa d'élimination de l'archiviste ou proposé pour l'élimination par un service d'archives au service dont émanent les documents.
Document	Objet constitué d'un support et de l'information qu'il porte, considéré comme un tout signifiant.
Document engageant	Un document engageant est un document achevé et validé, produit ou reçu au nom d'une entreprise ou d'un organisme, qui contient une décision ou une information entraînant ou susceptible d'entraîner une incidence financière ou la responsabilité morale de son détenteur. Un document engageant doit être authentique, fiable et intègre.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Donnée	Mot, nombre, signal, chaîne de caractères, séquence de bits, morceau de matière ou tout autre élément brut enregistré dans un système d'information où il pourra être corrélé à d'autres objets et interprété pour constituer une information.
Fiche de paramétrage	Document contenant les informations nécessaires au paramétrage et au bon fonctionnement du SAE du Client ; ce document peut contenir des informations d'ordre fonctionnelles et/ou techniques selon un modèle fourni par le Client ou le Prestataire
Intégrité	Caractère complet et non altéré d'un document prouvant que celui-ci n'a subi aucun ajout, aucun retrait ni aucune modification, accidentelle ou intentionnelle, depuis sa validation.
Norme	Document de référence, souvent technique, parfois organisationnelle, approuvé par une instance de normalisation ou une autorité professionnelle qui formalise le déroulement d'un processus ou d'une opération dans le but de favoriser le développement économique.
Notice	Ensemble regroupant toutes les métadonnées descriptives associées au document archivé.
Original	Première rédaction définitive d'un document, engageant ou non, à partir de laquelle seront réalisées d'éventuelles copies ou reproductions.
Politique d'archivage	Déclaration, signée par la direction générale d'une entreprise ou d'un organisme et opposable à l'ensemble des collaborateurs, énonçant les principes de gouvernance et d'action pour se conformer à l'environnement réglementaire, répondre au besoin de mémoire et anticiper le risque de ne pas archiver et conserver certains documents.
Processus d'archivage	Ensemble des activités qui transforment les traces de l'activité d'une entreprise ou d'un organisme en un corpus cohérent d'objets documentaires fiables dont la non-disponibilité présenterait un risque. Le processus d'archivage croise les processus métier au moment de la déclaration des documents engageants et de leur entrée dans le système d'archivage, avec le contrôle de la qualité des documents archivés et la prise en charge de leur conservation matérielle.
Projet d'archivage	Ensemble des études, décisions et actions qui permettent à une entreprise ou un organisme de mettre en place une politique, un référentiel, des procédures et des outils de sorte que tous ses documents engageants soient sous contrôle, c'est-à-dire identifiés, sécurisés, conservés, accessibles, gérés tout au long de leur cycle de vie et détruits ou transférés aux archives historiques à échéance de leur durée de conservation.
Fonds	Séparation logique entre les archives (AIP) dans un même tenant.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

d'archives	Cette séparation sert à isoler des fonds d'archives par propriétaire. C'est un ensemble de documents de toute nature constitués de façon organique par un producteur dans l'exercice de ses activités et en fonction de ses attributions.
Référentiel de conservation	Document prescriptif qui, en application de la politique d'archivage, définit les durées de conservation des documents engageants d'une entreprise ou d'un organisme, en fonction des risques de non-disponibilité et des besoins d'accès à l'information, en précisant le sort final à échéance de ces durées.
Réplication	La réplication en « Y » consiste à dupliquer un document sur des stockages différents
Sécurité	Exigence d'un système d'archivage (électronique ou non) susceptible de comporter des documents dont il convient de contrôler l'usage (confidentialité, risque de divulgation) et/ou l'intégrité (non-modification des contenus, non altération des supports).
Support	Élément matériel sur lequel est enregistrée l'information pour produire un document et qui sert à la fois à le transmettre et à le conserver.
Traçabilité	Faculté de pouvoir présenter l'historique des traitements opérés sur un document durant tout le cycle de vie.
SIP	Paquet d'informations produit par le service producteur et transféré au SAE pour l'élaboration ou la mise à jour d'un ou plusieurs AIP et/ou de métadonnées. Un SIP est un paquet comprenant un fichier de métadonnées et les archives (documents binaires).
AIP	Paquet d'informations conservé dans un SAE, constitué d'un ou plusieurs documents numériques, de métadonnées techniques, de gestion et de description documentaire. Un AIP correspond à un enregistrement de la table DOCUMENT, 1 ou n documents associés, les métadonnées techniques de ces fichiers se trouvant dans la table CSDOCS.
DIP	Paquet d'informations transmis à un utilisateur ou un système de destination dans le cadre d'une procédure de communication en réponse à une requête au SAE. Le DIP est un export conforme aux exigences de la norme NF Z42-013. Il contient un ou plusieurs AIP (la ou les archives, les métadonnées techniques, descriptives et de gestion extraites des notices, les enregistrements des événements liés aux AIP qui se trouvent dans l'export ainsi que les empreintes liées à chaque objet numériques). Chaque DIP est lui-même signé et une attestation est produite à chaque génération.
DUA	La Durée d'Utilité Administrative (DUA) est la durée durant laquelle les documents d'archives doivent être conservés à des

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

	fins de consultation et d'utilisation, soit par ceux qui les ont produits, soit par des services d'archives. Durant cette durée minimale de conservation à respecter, les documents archivés ne peuvent être détruits
Workflow	Un workflow correspond à un ensemble de tâches à effectuer pouvant nécessiter ou non l'intervention d'un acteur
Service versant	Tout service administratif qui transfère des archives en sa possession dans un service d'archives, qu'il les ait lui-même produites (on parle alors de service producteur) ou qu'il les ait héritées d'un service dont il a ou non repris les attributions.
Service producteur	Personne physique ou morale, publique ou privée, qui a produit, reçu et conservé des archives dans l'exercice de son activité.
Service d'archive	Le service archive se charge de la gestion de l'archivage, c'est-à-dire de la collecte des documents d'archives, le contrôle de la tenue des archives courantes produites ou reçues, la conservation des archives intermédiaires, le tri, le classement, la description, et toute la rédaction des instruments de recherche et de la communication des archives.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

1 PRÉSENTATION GÉNÉRALE

1.1 Enjeux liés à l'archivage électronique

L'article L. 211-1 du Code du patrimoine définit les archives comme « *l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité.* »

L'archivage électronique commence dès la création des documents et permet à l'organisation productrice de l'information de les exploiter pendant toute la durée de leur cycle de vie. L'archivage est un processus dynamique comprenant plusieurs étapes nécessaires à son déroulement et son aboutissement. Il met en œuvre un ensemble d'actions, d'outils et de méthodes pour collecter, identifier, classer, conserver, communiquer et finalement détruire le cas échéant les contenus numériques. C'est un processus qui fait appel à de multiples domaines de la gouvernance informatique :

- La gestion électronique de documents pour la classification, l'indexation, la recherche multicritères, sémantique, plein-texte, etc. ;
- La sécurité des systèmes, l'interopérabilité, la preuve, la journalisation, la veille réglementaire ;
- Le stockage sur les infrastructures (matérielles et logicielles) ;
- Les outils de conservation à long terme du numérique, la veille technologique.

Les raisons d'archiver sont nombreuses :

- **Respecter des obligations réglementaires ou législatives** : les textes législatifs définissent le périmètre documentaire qui doit légalement être conservé à des fins de preuve, fournit les durées de conservation associées ainsi que les exigences spécifiques au domaine considéré. Les archives publiques sont principalement régies par le code du patrimoine ; pour les archives privées, chaque code fournit les informations sur la conservation des documents produits par les activités qu'il couvre (code du commerce, code du travail, code général des impôts, etc.).
- **Protéger des droits** : les documents archivés peuvent être utilisés dans le cadre de litiges et de règlement de contentieux. Les tribunaux considèrent désormais les documents électroniques comme des preuves recevables au même titre que les originaux papiers, à condition que leur conservation respecte les normes et réglementations. Plus largement, l'archivage des documents numériques garantit les droits des personnes, morales et physiques, en leur fournissant des preuves à tout moment (contrat, droit de propriété, droit à la retraite...).

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- **Maîtriser les risques et préserver la pérennité de l'activité** : l'archive est sécurisée et pérennisée, elle garantit l'accès aux contenus nécessaires à la continuité de l'activité en cas de sinistre.
- **Conserver la mémoire** : lorsque les documents revêtent un aspect historique ou patrimonial, l'archivage est le garant de la mémoire de l'organisation ou de la personne.
- **Faciliter l'exploitation des documents** : un archivage efficace et opérationnel permet de rendre les documents disponibles et exploitables dans les meilleures conditions.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

La politique d'archivage sécurise la gestion de l'information de l'établissement en réduisant les risques de perte de données ou les failles de sécurité. La politique d'archivage doit définir les points suivants :

- Les niveaux de service du service d'archivage aux utilisateurs construit sur le SAE ArchiveMi (type d'archivage, formats des documents, modalités de communication, durées de conservation, ...),
- Les fonctionnalités mises en œuvre (fonction de dépôt, de communication, de restitution, ...),
- Les principes de sécurité à respecter.

Dans le cas où le **Client** dispose de sa propre politique d'archivage, il s'assure de sa comptabilité avec le présent document établi par be ys trusted solutions France dans le cadre de l'offre SAE **ArchiveMi**.

1.2 Cadre normatif et réglementaire appliqué

Notre SAE **ArchiveMi** est conçu et exploité dans le respect strict des référentiels nationaux et internationaux garantissant la valeur probatoire des documents électroniques :

Normes ou Textes applicables	Explications
NF Z42-013 / NF 461	Respect des exigences techniques et organisationnelles de cette norme, garantissant l'intégrité, la pérennité, la traçabilité et la lisibilité des archives
ISO 27001:2022	Garantit un niveau de sécurité optimal pour la gestion de la confidentialité, intégrité et de la disponibilité des données

1.3 Cadre normatif et réglementation sectoriel applicables

Le **Prestataire** reconnaît que chaque **Client** peut être soumis à des obligations réglementaires spécifiques liées à son secteur d'activité. À ce titre, le **Prestataire** s'engage à évaluer systématiquement les impacts techniques, fonctionnels et sécuritaires de ces réglementations avant toute mise en application au sein du SAE.

Le Prestataire s'engage également à respecter la conformité décrite ci-après :

Normes ou Textes applicables	Explications
SIAF	Conformité avec les directives du SIAF (Service Interministériel des Archives de France)

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés **be ys trusted solutions France** - Toute reproduction ou diffusion même partielle interdite sans autorisation

1.4 Niveau de sécurité physique et informatique respecté

La sécurité des archives est assurée par un dispositif de défense en profondeur, détaillée dans la Politique de Sécurité de l'Information du **Prestataire** et consultable uniquement sur site.

Cette politique garantit :

- **Sécurité physique** : Hébergement dans des datacenters hautement sécurisés, certifiés ISO 27001 et HDS, disposant d'un contrôle d'accès strict ;
- **Sécurité Informatique** : Cloisonnement physique des données du Client avec chiffrement des flux et audits de vulnérabilité réguliers ;
- **Résilience** : Un plan de continuité d'activité (PCA) et de reprise d'activité (PRA) assurent la disponibilité des documents archivés même en cas de sinistre majeur.

Toutes ces mesures de sécurité sont synthétisées dans cette présente politique, au niveau du paragraphe 10 « **Sécurité de l'information** ».

1.5 Gestion de la politique **ArchiveMi**

1.5.1 Identification du document

La présente Politique d'Archivage est formellement identifiée par un identifiant d'objet unique, dit OID (Object Identifier). Cet identifiant numérique, structuré selon la hiérarchie internationale de l'ISO, permet de désigner de manière univoque et immuable le cadre normatif et organisationnel appliqué aux archives gérées par le Système d'Archivage Électronique (SAE).

L'OID de cette politique est : 1.3.6.1.4.1.62466.82.1.2.

Ce document constitue la politique officielle et la déclaration des pratiques du service ArchiveMi, fourni par be ys trusted solutions France, ci-après le **Prestataire**. Il décrit les engagements du **Prestataire** de services, en tant que Tiers Archiveur certifié NF461 et agréé SIAF (Service Interministériel des Archives de France).

1.5.2 Circonstances dans lesquelles l'OID doit être modifié

Toute modification de la présente politique ayant une incidence significative sur le service nécessite une mise à jour de l'OID, afin de permettre une distinction claire entre les différentes versions de la politique.

En cas de modification prévue de l'OID de la politique, cette dernière et son analyse d'impact sont soumises à la Direction du **Prestaire** pour approbation.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

2 OBJECTIFS D'UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE

Le Système d'Archivage Électronique (SAE) **ArchiveMi** a pour objectif principal de maintenir la valeur probatoire des documents numériques confiés. Ses caractéristiques fondamentales reposent sur les quatre piliers de la norme NF Z42-013 :

- **L'intégrité** : Absence de modification non autorisée, scellée par empreinte numérique ;
- **La pérennité** : Lisibilité des formats sur le long terme par une gestion active des supports et des fichiers ;
- **La sécurité** : Confidentialité des accès et disponibilité des données ;
- **La traçabilité** : Journalisation immuable de chaque événement du cycle de vie (versement, consultation, élimination).

Les principes mis en œuvre au sein du SAE doivent être en permanence conformes à ceux présentés dans cette politique d'archivage. De ce fait, nous effectuerons une mise à jour de cette politique d'archivage vis-à-vis des évolutions internes et/ou externes (demande(s) effectuée(s) par les clients). Cette politique d'archivage sera archivée dans notre propre SAE afin de garantir l'intégrité de ce document dans le temps.

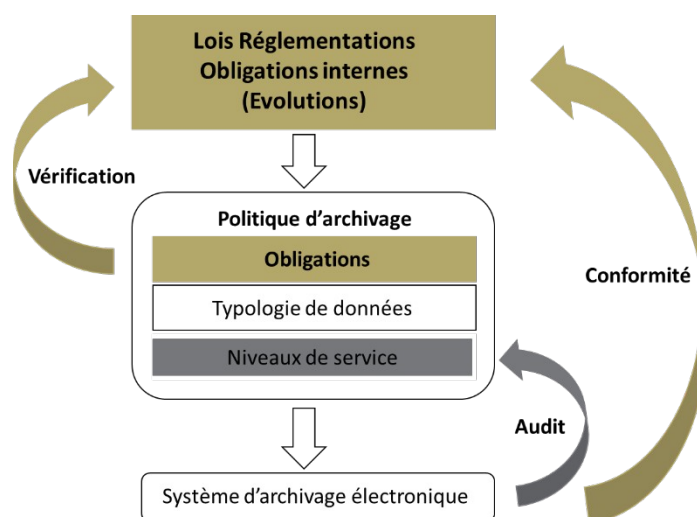


Figure 1 : Principe de la mise à jour de la politique d'archivage

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

3 PARTIES PRENANTES, RÔLES ET RESPONSABILITÉS

3.1 Le Client

Le client transfère des archives en sa possession dans le SAE ArchiveMi. Le client s'engage à fournir toutes les informations relatives à la nature et à la durée de vie de l'archive ainsi que leur éventuel caractère confidentiel et/ou les accès limités à be ys trusted solutions France. Le client est responsable de l'exactitude de ces informations et de leur bonne transmission. Pour préciser les conditions techniques mises en œuvre, le client et be ys trusted solutions France concluent un contrat précisant les conditions du traitement et en particulier le versement et les accès des archives.

3.2 Les utilisateurs client

Les utilisateurs représentent des personnes physiques et/ou des comptes de service qui souhaitent verser des documents et/ou consulter les informations conservées par le SAE ArchiveMi dans le respect des conditions légales, réglementaires ou contractuelles en vigueur. Les utilisateurs client doivent également respecter la confidentialité, le cas échéant, des archives traitées et ne pas tenter d'y accéder s'ils ne disposent pas des droits associés. Dans la mesure où l'utilisateur dispose d'un mode d'accès spécifique et personnel (authentification par identifiant/mot de passe, certificat ou autres), il s'engage à le conserver confidentiel et en faire un usage sous son contrôle exclusif. De même, les utilisateurs ne doivent pas tenter de détériorer tout ou partie du service d'archivage électronique sécurisé, du SAE et/ou de son contenu.

3.3 be ys trusted solutions France

be ys trusted solutions France est responsable de l'ensemble des prestations rendues par le service d'archivage électronique conformément à la politique d'archivage dont elle est l'origine. L'ensemble des prestations peut être décliné en plusieurs niveaux de sécurité – services détaillés dans le Contrat passé avec le **Client**. be ys trusted solutions France est également responsable des moyens mis en œuvre pour satisfaire les exigences définies dans la politique d'archivage.

be ys trusted solutions France accompagne le client dans l'élaboration du format attendu au niveau des métadonnées et des documents à archiver dans notre SAE. be ys trusted solutions France accompagne également le client en complétant avec lui une fiche de paramétrage nécessaire à l'ouverture du service d'archivage (volumétrie des documents à archiver, cloisonnement des données (physique ou logique), accès aux archives, etc.).

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Au sein de **be ys trusted solutions France**, plusieurs acteurs ont la charge du SAE :

- **Le Customer Success Manager (CSM)** : Personne en charge des relations contractuelles, du suivi du bon déroulement du Service de tiers archivage. Il s'assure du bon déroulement du Service d'archivage et du suivi du traitement de l'ensemble des demandes Client et correspond périodiquement avec le correspondant (ou référent) central du Service d'Archivage pour échanger sur tous ces points.
- **Le Service d'archivage** : Le Service d'archivage est l'entité destinataire du transfert et assurant la gestion des archives transférées par le Client et destinées à être communiquées aux différents utilisateurs, et, dans le respect des délais de communicabilité. Ce service inclut les rôles de Responsable Archivage, d'administrateur technique de la plate-forme ArchiveMi et d'experts applicatif, stockage et infrastructures.
- **Le Service support (hot-line)** : Ce service traite les demandes d'anomalie qui lui sont remontées via l'outil de ticketing. Cet outil est accessible par le correspondant (ou référent) central du Service d'Archivage et Le ou les Service(s) versant(s).

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

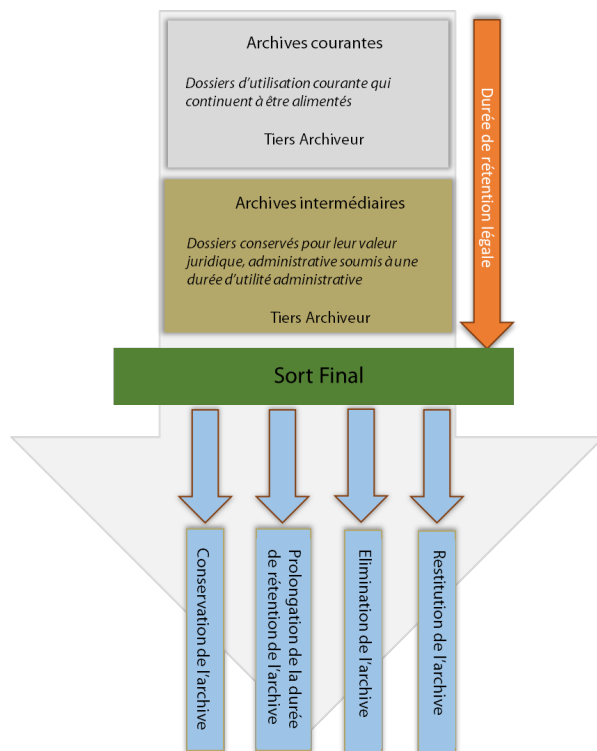
4 DIFFÉRENCE ENTRE ARCHIVES PRIVÉES ET ARCHIVES PUBLIQUES

L'archivage est un processus dynamique comprenant plusieurs étapes nécessaires à son déroulement et son aboutissement.

4.1 Cycle de vie des documents d'archives privées

Les archives privées en France sont l'ensemble des archives produites par toute personne, physique ou morale n'étant pas assimilé service ou organisme public français, ou n'exerçant pas une mission de service public pour le compte de l'administration publique ou territoriale.

La vie d'un document d'archives privées n'est pas linéaire.



Les documents d'archives privées ont un cycle de vie qui se décompose en plusieurs étapes successives jusqu'au sort final.

L'archive est dite "courante" lorsqu'elle est utilisée par les différents services dans leurs activités quotidiennes. Elle peut circuler entre les acteurs pour qu'ils en prennent connaissance et utilisent l'information dans des processus métier. La période couverte est appelée durée d'utilisation courante ou DUC, qui prend fin dès lors que le document n'est plus nécessaire aux processus qu'il a déclenchés où qu'il concerne.

L'archive est dite "intermédiaire" lorsqu'elle n'a plus d'utilisation courante mais doit être conservée pour des raisons juridiques ou réglementaires (disposer de

preuves, témoigner de droits, répondre à des contrôles...). Il est conseillé de conserver les archives intermédiaires dans un service d'archives (électronique lorsqu'il s'agit de documents et de données numériques) afin qu'elles soient classées, sécurisées et conservées dans les conditions et pour la durée requise. Sauf dérogation, son accès est alors restreint au service qui a produit le document et à ceux qui assurent sa gestion. Les conditions et la durée de conservation sont

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

définies par la législation en vigueur ou les exigences ou recommandations liées à la typologie documentaire.

A l'issue de la durée de rétention légale, l'archive est soumise à l'application du sort final souhaité par le client, à savoir :

- La prolongation de la durée de rétention de l'archive,
- L'élimination de l'archive,
- La restitution de l'archive avec toutes ses métadonnées et les différents journaux d'évènements,
- La conservation de l'archive dans le SAE.

Un référentiel de conservation paramétrable (typologie de document, durée de conservation, sort final) est alors renseigné avec le client grâce à notre fiche de paramétrage.

4.2 Cycle de vie des documents d'archives publiques

Les archives publiques en France sont l'ensemble des archives produites, reçues ou traitées par toute personne, physique ou morale, exerçant une mission de service public ou tout service ou organisme public français. Elles sont conservées par leurs administrations d'origine pour leur usage propre ou pour celui des citoyens français (par exemple, pour justifier de leurs droits), puis ultérieurement par les services d'archives publiques qui les mettent à disposition des historiens et des chercheurs.

La vie d'un document d'archives publiques n'est pas linéaire.

Les documents d'archives publiques ont un cycle de vie qui se décompose en trois phases successives.

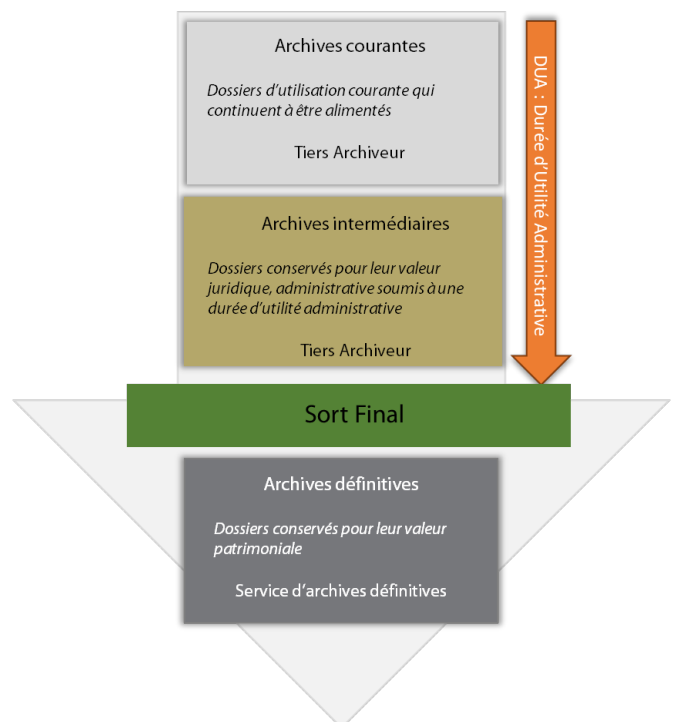
L'archive est dite "courante" lorsqu'elle est utilisée par les différents services dans leurs activités quotidiennes. Elle peut circuler entre les acteurs pour qu'ils en prennent connaissance et utilisent l'information dans des processus métier. La période couverte est appelée durée d'utilisation courante ou DUC, qui prend fin dès lors que le document n'est plus nécessaire aux processus qu'il a déclenchés où qu'il concerne.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation



L'archive est dite "intermédiaire" lorsqu'elle n'a plus d'utilisation courante mais doit être conservée pour des raisons juridiques ou réglementaires (disposer de preuves, témoigner de droits, répondre à des contrôles...). Il est conseillé de conserver les archives intermédiaires dans un service d'archives (électronique lorsqu'il s'agit de documents et de données numériques) afin qu'elles soient classées, sécurisées et conservées dans les conditions et pour la durée requise. Sauf dérogation, son accès est alors restreint au service qui a produit le document et à ceux qui assurent sa gestion. Les conditions et la durée de conservation sont définies par la législation en vigueur ou les exigences ou recommandations liées à la typologie documentaire.

A l'issue de la DUA (durée d'utilité administrative), l'archive est soumise à une règle de sort final qui détermine si elle peut être détruite ou si elle doit être conservée parce que l'information revêt un intérêt historique ou patrimonial. Ce contrôle est du ressort de la personne en charge du contrôle scientifique et technique après autorisation sollicitée par le Client via un bordereau d'élimination. Si l'archive est conservée, elle entre dans la troisième et dernière étape de son cycle de vie et devient une "archive définitive". Elle est alors conservée dans un service d'archivage définitif.

Un référentiel de conservation paramétrable (typologie de document, durée de conservation, sort final) est alors basé sur les directives et circulaires des Archives de France.

4.3 Gestion du cycle de vie

Le service d'archivage de be ys trusted solutions France est en mesure de gérer le cycle de vie des archives depuis leur versement jusqu'à leur élimination ou leur transfert en archive définitive. Pour cela, le service d'archivage de be ys trusted solutions France utilise un référentiel de conservation paramétrable permettant de définir pour chaque typologie de document la durée de conservation et le sort final du document (élimination ou transfert en archive définitive).

Nous utilisons notamment pour cela :

- Un référentiel de conservation paramétrable (typologie de document, durée de conservation, sort final) renseigné grâce à notre fiche de paramétrage,
- Une traçabilité complète des actions et événements survenus.

En fonction du sort final du document, notre service d'archivage permet :

- Dans le cas d'archives publiques le « sort final » est du ressort de l'entité en charge du contrôle scientifique et technique des archives compétentes (Archives départementales, Archives nationales, ...),
- Dans le cas d'archives privées le transfert vers le **Client** afin que ce dernier conserve les archives déterminées,

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Soit l'élimination de l'archive.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

5 COMPOSITION DES SIP (PAQUETS EN ENTRÉE)

5.1 Organisation des documents d'archives dans le SIP

Nous remplissons avec vous, lors d'ateliers fonctionnels, une fiche de paramétrage et un document de compte-rendu qui détaillent les éléments vus pendant ces différents ateliers. Ces derniers permettent de poser à plat les attentes. Grâce à cela, nous nous engageons à offrir un service de qualité tout en répondant à vos attentes.

Pendant ces ateliers, nous voyons les aspects suivants :

- Un atelier de présentation globale de notre SAE sans aucune spécificité ;
- Plusieurs ateliers fonctionnels pour échanger sur les points suivants :
 - o Gestion du plan de classement ;
 - o Gestion des utilisateurs et des habilitations ;
 - o Processus de versement ;
 - o Processus de communication ;
 - o Processus d'élimination ;
 - o Processus de restitution d'une ou plusieurs archives ;
 - o Processus de réversibilité.
- Plusieurs ateliers techniques pour échanger sur les ouvertures de flux entre notre SI et celui du client, utilisation d'un SSO ou non, etc.

5.2 Organisation des métadonnées dans le SIP

Les métadonnées relatives aux archives électroniques sont catégorisées selon trois catégories :

- **Les métadonnées de description.** Ces métadonnées sont saisissables par un utilisateur. Ces dernières sont modifiables. L'utilisateur décrit son versement (intitulé, description, support utilisé) et détermine la typologie associée (activité, rubrique, sous-rubrique et typologie) ;
- **Les métadonnées de gestion.** Ces métadonnées sont également saisissables par un utilisateur. Ces dernières sont modifiables. L'utilisateur détermine la date à partir de laquelle la ou les archives doivent être conservées ;
- **Les métadonnées techniques.** Ces métadonnées sont alimentées automatiquement par notre SAE ArchiveMi (nom du fichier, taille, format, chemin de stockage, etc.) ainsi que la signature calculée par le SAE ArchiveMi. Ces dernières sont affichées mais non modifiables par un utilisateur.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Par défaut, le SAE de be ys trusted solutions France propose un certain nombre de métadonnées (celles mentionnées ci-dessous). Ces dernières peuvent être complétées pour répondre aux besoins du **Client**.

Public

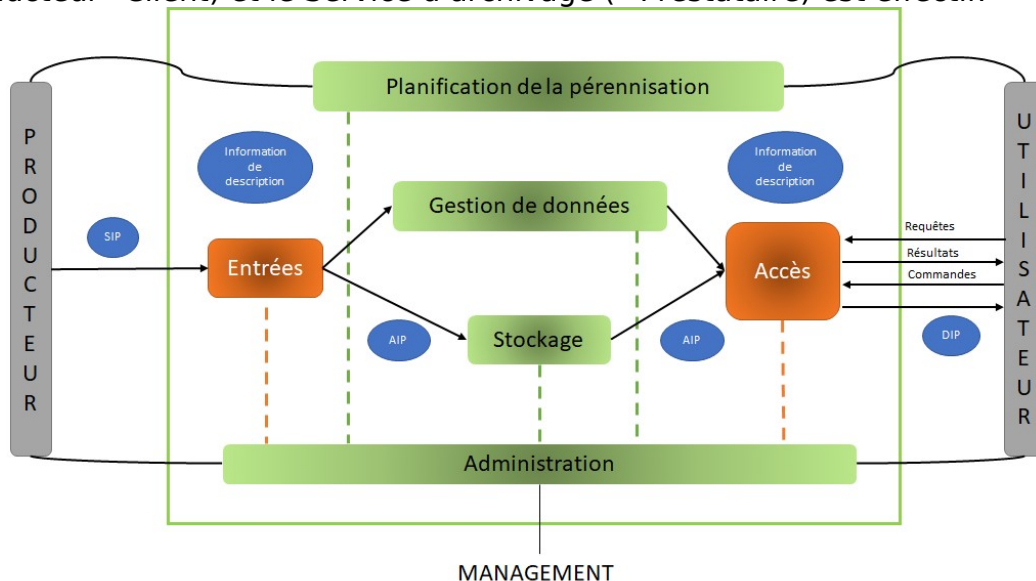
be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

5.3 Transfert entre le Service Versant et le Service d'Archivage

Le processus de versement débute par l'envoi des objets à archiver depuis le service versant (= Producteur), et se termine par la production de l'attestation d'archivage par notre SAE. Lorsque le versement est achevé, le transfert de responsabilité de conservation des archives électroniques entre le service versant (=Producteur=Client) et le Service d'archivage (=Prestataire) est effectif.



be ys trusted solutions France conseille de produire et de verser des documents dans un format normalisé ou dans un standard utilisable librement afin de minimiser :

- D'une part les risques d'altération d'intégrité liés à d'éventuelles opérations de conversion ;
- D'autre part les risques sur l'exploitation sur le long terme de documents dans un format non normalisé ou non conforme aux normes et standards préconisés.

Lors du versement d'un document archivé, les AIP sont déposés dans les composants de conservation de production de chacun de nos sites de conservation. be ys trusted solutions France ne procède à aucune copie des données du **Client** d'un environnement à un autre sans l'accord au préalable de ce dernier. Cet accord peut être formulé :

- Soit depuis notre outil de ticketing ;
- Soit depuis la réception d'un courriel.

Aucune copie ne sera effectuée sur un accord oral.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Lors de la validation du versement, une attestation est générée automatiquement et instantanément puis attachée au versement lui-même. Cette attestation est au format XML et accessible depuis le versement lui-même, elle contient les informations sur le versement (Producteur, Service versant ...) ainsi qu'une description de chaque fichier versé. Pour chaque fichier, l'attestation contient les métadonnées techniques (nom, taille, chemin de stockage) ainsi que la signature calculée par notre SAE.

5.4 Gestion des métadonnées

Le service d'archivage de be ys trusted solutions France accompagne afin que chaque versement se déroule correctement en transmettant les métadonnées au bon format et les documents à archiver correspondant à notre SAE.

Notre SAE **ArchiveMi** dispose pour le moment des métadonnées suivantes pour la gestion des archives :

Métadonnées	Obligatoire	Commentaires
Intitulé	Oui	Texte libre
Description	Non	Texte libre
Activité	Oui	Une fois la typologie sélectionnée, l'activité correspondante du référentiel s'affiche automatiquement
Rubrique	Oui	Une fois la typologie sélectionnée, la rubrique correspondante du référentiel s'affiche automatiquement
Sous-rubrique	Oui	Une fois la typologie sélectionnée, la sous-rubrique correspondante du référentiel s'affiche automatiquement
Typologie	Oui	Liste déroulante pour catégoriser la ou les différentes archives
Confidentialité	Oui	Hérité automatiquement du type de document sélectionné : • Public : visible par tout le monde • Service : visible uniquement par le service du créateur et les services/utilisateurs habilités à consulter les objets du service courant • Confidentiel : visible uniquement par le créateur
Date du document	Oui	Date du document
Support	Oui	Liste déroulante pour sélectionner le type (Electronique ou Physique)

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Type de support physique	Oui s'il agit d'une archive physique	Permet de définir le type du support (CD, DVD, Affiche, Maquette, ...)
Début durée de conservation	Oui	Date à partir de laquelle l'objet doit être conservé pour obéir aux exigences réglementaires, pour prévenir les risques de non-disponibilité des documents et/ou pour répondre aux besoins de mémoire de l'entreprise

Les métadonnées présentes dans le tableau ci-dessus sont considérées comme « standards ». Cette liste peut être revue avec le **Client** lors des ateliers fonctionnels.

A ces métadonnées, notre SAE **ArchiveMi** rajoute automatiquement les informations suivantes :

Intitulé	Type	Commentaire
Service versant ou le Client	Texte	Information récupérée selon l'utilisateur ayant procédé au versement
Le sort final	Texte	Récupérer selon la typologie sélectionnée
La communication	Booléen (oui ou non)	Récupérer selon la typologie sélectionnée
La notion « Elimenable »	Booléen (oui ou non)	Récupérer selon la typologie sélectionnée
Confidentialité	Liste	Hérité automatiquement de la typologie sélectionnée : • Public : visible par tout le monde • Service : visible uniquement par le service du créateur et les services/utilisateurs habilités à consulter les objets du service courant • Confidentiel : visible uniquement par le créateur
L'empreinte calculée du document versé	Alphanumérique	Oui
Date d'élimination finale	Date (TimeStamp ISO 8601)	Calculée en fonction de la typologie sélectionnée et à partir de la date de début durée de conservation

5.5 Indexation des documents

Notre SAE ArchiveMi permet d'indexer le document archivé avec ses métadonnées. De façon optionnelle, nous utilisons aussi une indexation « texte intégral ». Ceci a pour but d'indexer à la fois les métadonnées mais aussi le contenu du document

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

archivé si le contenu est accessible. L'indexation du contenu du document ne pourra pas s'effectuer pour les fichiers étant protégés par un mot de passe ou selon le format.

5.6 Formats d'archivage

5.6.1 Liste des formats autorisés

Afin de garantir la lisibilité des documents archivés dans le temps, nous acceptons, par défaut, les formats suivants :

- Les documents PDF ;
- Les documents Texte (.txt).

La liste présentée ci-avant n'est pas exhaustive et pourra être adaptée en fonction des besoins spécifiques du **Client**, afin d'accepter d'autres formats ou bien d'en réduire la liste (par exemple, ne prendre en compte que les formats PDF uniquement). Cette partie sera traitée dans le Contrat associé et dans la fiche de paramétrage.

be ys trusted solutions France n'effectue aucune conversion des formats avant le versement. Le **Client** doit s'assurer et respecter les formats présents dans la fiche de paramétrage.

5.6.2 Mécanisme de contrôle du format

Le contrôle du format des documents archivés est réalisé à l'aide de l'API Aspose et plus précisément via le produit Aspose.PDF qui permet de créer ou d'éditer des documents au format PDF. Cette API implémente les contraintes de structures (RFC) des différents formats fichiers.

Pour le contrôle des fichiers ZIP, notre SAE ArchiveMi utilise la librairie standard java java.util.zip.

La vérification du format des fichiers s'effectue via un trigger qui est activé sur la table contenant les documents archivés et qui s'appuie sur l'API Aspose. Cette API permet de tester notamment les formats suivants : **pdf, xls,xlsx, doc, docx, ppt, pptx, xml, zip**.

En fonction du format du fichier l'API effectue les vérifications suivantes :

- Pour les fichiers PDF et Office ;
- Pour les fichiers XML : l'API essaie d'ouvrir le fichier avec un parseur xml (**check.xml(...)**) ;
- Pour les fichiers compressés ZIP : l'API essaie de lire l'arborescence du ZIP.

Cette liste n'est pas exhaustive.

Lors du versement d'un document, notre SAE ArchiveMi vérifie que le format du document à archiver correspond bien à celui qu'il prétend être. Si le document n'est

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

pas conforme au format prétendu, ce dernier n'est pas archivé. Le service versant en sera immédiatement informé soit par retour de webservice soit directement par les interfaces graphiques de notre SAE.

5.7 Conversion dans un format plus pérenne

Sur le long terme, la prévention contre l'obsolescence technologique est fondamentale. Cette obsolescence se manifeste à plusieurs niveaux : obsolescence des supports, obsolescence des technologies du système, obsolescence des formats de fichiers.

Un format de fichier peut en effet, durant son cycle de vie, devenir obsolète pour diverses raisons :

- Les nouvelles versions d'un logiciel ne prennent pas en charge les fichiers des versions antérieures ;
- Le format lui-même est supplanté par un autre ou devient plus complexe ;
- Le format est peu adopté, ou peu de logiciels compatibles sont créés ;
- Le format échoue, stagne ou n'est plus compatible avec l'environnement informatique actuel ;
- Le logiciel qui prend en charge le format n'arrive pas à percer le marché ou est acheté par un concurrent qui le retire du marché.

Un format en voie d'obsolescence correspond à un format dont les caractéristiques sont en passe de ne plus correspondre aux critères requis pour l'archivage pérenne. Il faut détecter lors des opérations de veille technologique, ces formats qui devront être rapidement convertis vers de nouveaux formats pérennes.

Il existe plusieurs typologies de formats :

- Un format peut être spécifié, c'est-à-dire suffisamment bien décrit pour en développer une implémentation ;
- Un format peut être ouvert : la convention est publique, sinon, on dit que le format est fermé. En France cela est codifié dans une loi du 21 juin 2004 ;
- Un format peut être normalisé : un ensemble d'association s'entendent pour adopter la convention et l'utiliser ;
- Un format peut être standardisé : il est très utilisé et de ce fait il est reconnu comme standard ;
- Un format peut être propriétaire. il dépend de l'existence d'un propriétaire qui peut choisir de l'ouvrir ou non ;
- Un format peut être dérivé d'autres formats (le HTML vient par exemple du SGML).

En respect de la norme NF Z42-013, notre SAE ArchiveMi utilise uniquement les formats « normalisés » ou « standardisés ». L'équipe en charge du SAE ArchiveMi

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

est sensibilisée à cette question de l'obsolescence des formats et agit donc sur plusieurs plans :

- Contrôler les formats des fichiers qui entrent dans notre SAE ;
- Effectuer une veille technologique sur tous les formats présents dans le SAE permettant ainsi de détecter les formats obsolètes.

Ceci permet :

- De vous conseiller sur le choix des meilleurs formats d'archivage au moment du versement ;
- De vous avertir lorsque nous détectons que certains fichiers conservés dans notre SAE ont un format en voie d'obsolescence ;
- De vous conseiller lors d'une détection de format en voie d'obsolescence :
 - o Soit en convertissant après accord de votre part les archives dans un format plus pérenne ;
 - o Soit en vous restituant les archives si vous ne souhaitez pas procéder à la conversion.

Le service d'archivage de be ys trusted solutions France limite, par défaut, les formats supportés dans son SAE afin de minimiser le risque d'obsolescence des formats. Le format TXT est un format très simple qui présente peu de risques d'obsolescence et le format PDF est en revanche un format plus riche (ISO 32000).

Cependant, notre SAE ArchiveMi dispose d'un service de conversion intégré de documents, qui ne nécessite aucune installation ou configuration particulière. Ce service permet d'effectuer des conversions afin de pérenniser les documents archivés dans le temps (par exemple de convertir un format PNG vers un format PDF/A), en conservant le document original ainsi que le document converti. Cette option peut être activée selon les attentes du **Client**.

5.8 Veille technologique et lutte contre l'obsolescence des formats

Le **Prestataire** garantit la lisibilité à long terme des documents confiés en mettant en œuvre une stratégie proactive de lutte contre l'obsolescence logicielle et matérielle. Cette démarche repose sur trois piliers :

- **Sélection rigoureuse à l'entrée** : Le SAE privilégie l'utilisation de formats de fichiers ouverts, documentés et pérennes (tels que le PDF/A, XML, ou TIFF). Le **Prestataire** conseille le **Client** dès la phase de versement sur les formats offrant les meilleures garanties de stabilité dans le temps ;
- **Veille active et technologique** : Le **Prestataire** réalise une veille permanente sur l'évolution des standards du marché et des outils de lecture. Cette veille vise à identifier précocement les formats risquant de devenir illisibles (formats propriétaires, fin de support éditeur) ;

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- **Stratégie de préservation** (Migration) : En cas d'obsolescence avérée ou imminente d'un format, le **Prestataire** s'engage à proposer et à mettre en œuvre des opérations de migration de support ou de conversion de format (transcodage). Ces opérations sont réalisées de manière à préserver l'intégrité du contenu informationnel et sont intégralement tracées dans le journal de cycle de vie de chaque archive concernée, garantissant le maintien de la valeur probatoire malgré le changement de format technique.

5.9 Intégrité des archives

Selon les normes NF Z42-013 et ISO 14641, l'archivage électronique est un domaine distinct qui porte sur la conservation à moyen ou long terme de l'intégrité d'une information d'un document. L'information d'intégrité fournit les moyens de contrôler que le contenu numérique n'a pas été altéré au cours du temps.

Notre SAE ArchiveMi procède au contrôle d'intégrité tout au long de la conservation du (des) document(s) archivé(s) sans attendre des migrations éventuelles ou l'interrogation par les utilisateurs. be ys trusted solutions France a mis en place des dispositifs de vérification d'intégrité basés sur l'empreinte des documents archivés. Pour cela, nous comparons l'empreinte du document archivé avec celle conservée dans les journaux de cycle de vie.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

6 GESTION DU CYCLE DE VIE

6.1 Application du sort final

6.1.1 Cas des archives privées

Une fois la durée de vie d'une archive échue, trois cas de figure sont possibles :

- Le **Client** souhaite conserver plus longtemps l'archive. Dans ce cas, l'archive est prolongée par rapport à la demande du **Client** ;
- Le **Client** ne souhaite pas conserver l'archive et demande ainsi son élimination. Dans ce cas, la procédure d'élimination est initiée et une attestation de suppression est transmise au **Client** ;
- Le **Client** ne souhaite pas conserver l'archive et demande qu'elle lui soit restituée. Dans ce cas, la procédure de restitution d'une archive est initiée et l'ensemble des informations (métadonnées, document archivé, différents journaux) est restitué au **Client**.

Les procédures (élimination et restitution) sont réglementées en raison du caractère irréversible : les données qui ont été détruites ne peuvent plus être reconstituées. Toute élimination d'archives privées doit donc faire l'objet d'un visa préalable du **Client**.

6.1.2 Cas des archives publiques

Une fois la durée d'utilité administrative des documents échue, deux cas de figure sont possibles lorsqu'il s'agit d'archives publiques :

- Les documents présentent un intérêt administratif très long et/ou historique : ils doivent être versés au Service d'archives public territorialement compétent ;
- Les documents ne présentent ni intérêt administratif ni intérêt historique : ils peuvent être détruits. C'est cette dernière catégorie de documents qui est concernée par la procédure d'élimination.

La procédure est réglementée en raison de son caractère irréversible : les données qui ont été détruites ne peuvent plus être reconstituées. Toute élimination d'archives publiques doit donc faire l'objet d'un visa préalable de l'autorité chargée du contrôle scientifique et technique.

Cette autorisation doit être sollicitée par le **Client** via un bordereau d'élimination à faire viser par l'autorité en charge du contrôle scientifique et technique. Une copie de ce bordereau sera exigée par nos services avant toute suppression d'archives publiques.

6.2 Gestion de l'élimination des archives

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

L'élimination de documents d'archives est la procédure qui consiste à détruire les documents dont la conservation ne se justifie plus. L'élimination découle du délai de conservation qui se traduit par la date d'élimination calculée automatiquement.

Notre SAE **ArchiveMi** dispose d'un Workflow d'élimination afin de contrôler et bloquer des tentatives d'élimination. Notre SAE propose, pour chacun de ces processus, des écrans personnalisés permettant de réaliser toutes les actions disponibles. L'acteur peut ainsi interagir avec l'objet d'archives en cours de traitement avant de demander au Workflow de passer à la tâche suivante.

6.2.1 Traitement des archives à éliminer par le Client

6.2.1.1 Introduction

Le Client, s'il le souhaite, peut effectuer les actions suivantes :

- Lister les archives dont la date d'élimination arrive à échéance ;
- Editer le bordereau d'élimination et le transmettre si besoin à l'autorité chargée du CST dans le cas des archives publiques ;
- Procéder aux actions souhaitées (prolongation de la durée de vie, suppression ou transfert en archive définitive) ;
- Editer une attestation d'élimination en cas de suppression d'archives.

6.2.1.2 Application du sort final par le Client

En cas de transfert de l'archive vers le Client

Lorsque le Client ne souhaite pas supprimer l'archive présente dans le SAE du Prestataire mais souhaite néanmoins la récupérer, le Client procédera à une demande de restitution de ladite archive selon la procédure mentionnée ci-dessous.

En cas de prolongation

Le Client procède à la prolongation des différentes archives en indiquant la nouvelle date de prolongation. Dans ce cas, une nouvelle date d'élimination sera automatiquement recalculée par rapport à la date de prolongation renseignée par le Client.

En cas de suppression

Lorsque le Client souhaite supprimer une ou plusieurs archives, ce dernier doit rechercher et sélectionner les unités d'archives à supprimer. Dès lors que les unités d'archives ont été sélectionnées, le Client doit initier un bordereau d'élimination et demander sa validation en interne. Dès validation du bordereau par le Client, les unités d'archives sont immédiatement supprimées du SAE et une attestation d'élimination est automatiquement générée et conservée dans le SAE pour traçabilité.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.2.2 Délégation des archives à éliminer au Prestataire

6.2.2.1 Introduction

Nous présentons dans cette section la procédure de suppression d'une archive à la suite de la validation du Client. L'action de suppression vise à traiter les archives arrivant en fin de Durée d'Utilité d'Administrative. Le traitement de ce processus peut être réparti en trois temps :

1. Le mois précédant la fin de leurs durées de conservation, le Prestataire liste les archives éligibles et les soumet au Client.
2. La première quinzaine du mois suivant la réception de la demande de validation, le Client doit retourner au Prestataire la liste des archives avec le sort final à appliquer (suppression, prolongation, archive définitive) pour chacune des archives éligibles. Sans ce visa, aucune suppression ne sera autorisée.
3. Le dernier temps consiste à appliquer les instructions décrites dans un bordereau de suppression ou de destruction fourni par le Client au plus tard à la fin de la seconde quinzaine du mois :
 - a. Prolonger la durée de conservation, à mettre en œuvre sur la dernière quinzaine du mois.
 - b. Supprimer l'archive, appliquer le sort final, consiste à confirmer la suppression définitive proposée par le SAE et correspondant en tous points au bordereau de suppression validé par le Client.
 - c. Informer le Client de la bonne exécution du traitement.

La suppression consiste à détruire définitivement les archives du SAE du Prestataire sur l'ensemble des espaces de stockage, néanmoins des métadonnées sont conservées pour garder trace de l'existence passée d'une archive, de sa date de suppression et de la justification de sa suppression.

6.2.2.2 Initialisation du processus d'élimination

Le Prestataire adressera par courriel avec accusé de réception un bordereau d'élimination au Client indiquant la liste des archives devant être supprimées. A réception de ce courriel, le Client prendra connaissance de son contenu et désignera l'action à effectuer (suppression, prolongation, restitution) de chacune des archives listées.

6.2.2.3 Réponse du Client

Le Client adressera le formulaire de suppression par courriel (incluant les éléments attestant de l'accord de l'ensemble des responsables) au Prestataire. Cette

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

demande retournée par le Client sera archivée dans le SAE propre au Prestataire afin de respecter les normes en vigueur sur l'archivage électronique.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés **be ys trusted solutions France** - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.2.2.4 Application du sort final par le Prestataire

En cas de conservation de l'archive après sa durée légale de conservation

Lorsque le Client souhaite conserver l'archive même après sa durée légale de conservation dans notre SAE. Dans ce cas, l'archive sera automatiquement déplacée dans une table afin d'être conservée jusqu'à la demande de suppression formulée par le Client. Cette action de déplacement est gérée par un trigger qui vérifie si des archives ont une date d'élimination antérieure à la date du jour.

En cas de transfert de l'archive vers le Client

Lorsque le Client ne souhaite pas supprimer l'archive présente dans le SAE du Prestataire mais souhaite néanmoins la récupérer, le Prestataire procèdera à la restitution de ladite archive selon nos procédures en vigueur. Le Prestataire attendra la validation du Client afin de procéder à la suppression définitivement de la liste des archives restituées.

En cas de prolongation

Le Prestataire procèdera à la prolongation des différentes archives devant être prolongées selon nos procédures en vigueur. Dans ce cas, une nouvelle date d'élimination sera automatiquement recalculée par rapport à la date de prolongation demandée par le Client.

En cas de suppression

Après l'accord du Client pour supprimer une ou plusieurs archives, le Prestataire procèdera à la suppression définitive des différentes archives selon nos procédures en vigueur.

6.2.3 Finalisation du traitement

Une fois les traitements effectués par le Prestataire, la finalisation consiste à informer le Client de la bonne exécution de la demande de suppression (supprimer, prolonger ou restituer). Pour cela, le Prestataire adressera soit un courriel avec accusé de réception et confirmation de lecteur ; soit une lettre recommandée avec accusé de réception au Client pour clore cette activité. Ce document récapitulera l'ensemble des archives traitées par le Prestataire et le sort appliqué avec la date d'action et éventuellement l'identifiant du journal pour confirmer la bonne suppression des archives.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

6.3 Gestion de la restitution des archives

La restitution permet donc au propriétaire d'archives de récupérer les unités d'archives qu'il souhaite, avant la fin de la DUA, entraînant ainsi leur élimination du SAE **ArchiveMi**. Ce processus de restitution peut être résumé en trois phases :

1. Création des bordereaux de restitution ;
2. Acquittement de la restitution ;
3. Confirmation de la destruction.

6.3.1 *Mode opératoire*

6.3.1.1Création du bordereau de restitution

Notre SAE permet au **Client** de rechercher et de sélectionner les unités d'archives à restituer. Dès lors que les unités d'archives ont été sélectionnées, le **Client** doit initier un bordereau de restitution en indiquant un motif et le transmettre au **Prestataire** pour traitement.

Cependant, si le **Client** ne souhaite pas effectuer cette action depuis notre SAE, peut utiliser son propre formulaire dès lors qu'il reprend l'ensemble des informations attendues. Dans ce cas, le **Client** transmet par courriel ou par notre solution de ticketing, la demande de restitution d'une ou plusieurs unités d'archives auprès du **Prestataire** pour traitement.

6.3.1.2Traitement et acquittement de la restitution

Dès réception du bordereau de restitution, le **Prestataire** s'engage à traiter la demande formulée par le **Client** en récupérant l'ensemble des unités d'archives (documents, métadonnées) souhaitées.

Le **Prestataire** transmet par un canal sécurisé (coffre-fort électronique, disque chiffré, ...) et selon la volumétrie les unités d'archives (documents et métadonnées) demandées par le **Client**.

Le **Prestataire** demande au **Client** un acquittement des unités d'archives récupérées par courriel afin d'attester que ces dernières ont bien été retournées au **Client**.

6.3.1.3Confirmation et destruction des unités d'archives

Dès confirmation de la bonne réception des unités d'archives restituées par le **Client**, le **Prestataire** s'engage à éliminer du SAE les unités d'archives restituées selon la procédure en vigueur. Une fois l'élimination effective, une attestation

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

d'élimination est automatiquement générée et conservée dans le SAE du **Client** pour traçabilité. Le **Prestataire** informe le **Client** de la bonne suppression.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

7 GEL / DÉGEL DES ARCHIVES

7.1 Introduction

On peut vouloir geler une archive pour diverses raisons, qui sont, de manière générale, constitutives de contentieux. Toute archive ayant valeur probatoire peut prétendre à ce type d'action, afin d'être rendue disponible pour les procédures juridiques et légales la concernant ou sur lesquelles elle peut faire preuve.

Une procédure de contentieux, dans le cadre d'un système d'archivage électronique (SAE), est susceptible d'engendrer les cas suivants :

- La justice a besoin de consulter certains documents : procédure de communication à un tiers ;
- La justice désire consulter les originaux des documents : procédure de restitution partielle ;
- Des documents du SAE sont fortement impliqués par le contentieux et doivent être préservés de toute altération de leur intégrité, donc de toute modification et de tout type de destruction : procédure de gel et de dégel.

Le gel est une procédure de précaution, notamment quant aux processus d'éliminations d'archives dont les durées d'utilité administrative sont échues, et dont le sort final est l'élimination.

7.2 Geler une archive

La procédure est appliquée uniquement par le **Client** ou par le service d'archivage de be ys trusted solutions France à la suite d'une demande écrite soit par courriel ; soit via notre outil de ticketing. Dans le cas d'un traitement de gel par le service de be ys trusted solutions France, aucune action ne sera effectuée par voie orale.

Geler une archive signifie donc qu'on suspend tout déroulement de son cycle de vie et toute action sur lui. Une archive gelée sera disponible à la consultation, communicable par dérogation, mais ne pourra être soumise aux processus listés ci-dessous :

- **Élimination** : une élimination en cours sera annulée par l'action de gel. Un dégel remettra l'archive au statut Conservée ;
- **Restitution** : la restitution entraînant l'élimination de la copie de l'archive contenue dans le SAE, même une restitution en cours ne pourra être menée à terme. Au dégel, l'archive sera à nouveau dans le statut Conservée ;
- **Transfert sortant** : ce processus versant l'archive dans un autre SAE amènera à la destruction de la copie de l'archive contenue dans le SAE où l'archive a été gelée. De fait, un transfert sortant en cours sera également annulé, le dégel passant l'archive dans le statut Conservée ;

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- **Communication** : une archive gelée ne doit pas pouvoir être communicable par erreur. Ainsi sa durée de communicabilité sera suspendue, mais elle pourra tout de même être communiquée à un tiers pour contentieux.

Dans le même ordre d'idée, toute modification des règles de gestion des archives gelées sera impossible. Ainsi, on ne pourra modifier ni la règle de communicabilité, ni la règle de conservation, et la possibilité de conversion sera également suspendue. Toute vérification d'intégrité reste possible.

Une fois le gel effectué par le service d'archivage de be ys trusted solutions France, ce dernier en informera le **Client** de la bonne prise en compte de la demande.

7.3 Dégeler une archive

La procédure de contentieux achevée, il faut procéder au dégel des différentes archives, afin de leur faire reprendre le cours de leur cycle de vie là où elles se sont arrêtées, en autorisant de nouveau leur prêt et leur éventuelle destruction.

Le **Client** peut procéder au dégel d'une archive, un motif sera demandé par notre SAE ArchiveMi lors du dégel afin de le tracer conformément à la norme en vigueur. Si le **Client** ne souhaite pas procéder au dégel, ce dernier peut solliciter le service d'archivage de be ys trusted solutions France à la suite d'une demande écrite soit par courriel ; soit via notre outil de ticketing en stipulant le motif associé au dégel. Une fois cette communication effectuée, be ys trusted solutions France pratiquera au dégel des archives en question et en informera le **Client** de la bonne prise en compte de la demande.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

8 TRAÇABILITÉ

La traçabilité des documents revêt une importance capitale be ys trusted solutions France s'efforce donc de tout mettre en œuvre afin d'offrir à ses **Clients** une traçabilité parfaite de l'activité autour de leurs archives, tout en sécurisant au mieux leur accès.

Les journaux, en tant que données, font l'objet d'un niveau de protection adapté au niveau de sensibilité.

Notre SAE ArchiveMi utilise deux types de journaux (le journal « workspace » et « tenant ») afin de lister toutes les opérations et ainsi garder l'historique des actions sur les documents archivés (versement, recherche, consultation, suppression, etc.) mais également sur les actions menées sur notre SAE ArchiveMi (arrêt/démarrage du serveur, connexion des utilisateurs, etc.).

Ces journaux sont générés à l'aide de traitement batch (ou scheduler) mis à disposition par notre SAE.

Le journal des événements est généré tous les jours à partir de 22h00 (celui du jour « J » qui prend en compte la journée de 24h de J-1 22h à J 22h).

Le journal du cycle de vie des archives est généré tous les jours à partir de 01h00 (celui du jour « J-1 »).

Journal des événements :

Ce journal comporte les informations liées au démarrage et à l'arrêt du serveur d'applications, aux connexions utilisateurs et aux échecs. Les traces associées à la création des notices documentaires figurent dans ce type de journal.

Journal de cycle de vie des archives :

Ce journal retrace toutes les étapes de cycle de vie liées aux documents archivés, éliminés, restitués durant la journée passée, ainsi que les modifications sur les profils d'archivage. Les traces liées à l'attachement des fichiers aux notices documentaires (archivage des documents) se trouvent dans ce journal.

Ils sont archivés sur l'espace de stockage via la réplication en Y mise en place. Les journaux associés aux documents archivés sont conservés dans les mêmes conditions de sécurité et de pérennité que les archives. Les journaux du cycle de vie des archives sont conservés pendant toute la durée de la prestation.

L'ensemble de nos journaux sont chaînés.

Comment fonctionne le chaînage des journaux ?

Chaque journal contient les éléments d'identification du journal précédent dans un bloc en entête de journal, afin d'assurer le chaînage des journaux. Le chaînage des journaux est assuré lors de la génération des journaux. Il s'effectue selon le processus suivant :

- Empreinte du journal à j-1,
- Date de clôture du journal,

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Contrôle de l'empreinte avec celle tracée lors de l'évènement du journal précédent.

Notre traçabilité permet de garantir le cycle de vie des archives, dans le respect des normes NF Z42-013 et ISO 14641.

9 EXHAUSTIVITÉ DES DOCUMENTS

Afin de respecter les exigences de la norme en vigueur be ys trusted solutions France doit mettre en œuvre un mécanisme de contrôle de l'exhaustivité des archives conservées prenant en compte les volumes entrants, conservés et sortants du SAE. Les opérations de contrôles d'exhaustivité sont enregistrées et les résultats non-conformes sont journalisés.

be ys trusted solutions France assure un contrôle de l'exhaustivité des archives à minima une fois par an voire une fois par mois. Pour procéder à ce contrôle, notre service d'archivage met en place des sondes qui viennent vérifier que notre SAE ArchiveMi n'a perdu aucune archive du Client. Cette sonde calcule automatiquement le nombre d'archives présentes et le compare avec les traces journalisées (nombre d'archives versées - nombre d'archives éliminées). En cas de différence, le service d'archivage be ys trusted solutions France est immédiatement prévenu et ce dernier s'engage à contacter dans la demi-journée le **Client** et à mettre en œuvre tous ses efforts pour remédier au problème.

Le **Client**, s'il le souhaite peut demander le résultat de chaque contrôle effectué.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

10 TION DE L'INFORMATION

SÉCURISA

10.1 Introduction et présentation de nos datacenters

Pour garantir la sûreté de l'information, nous avons fait le choix de **maîtriser totalement notre environnement informatique** : nous nous sommes ainsi rendus totalement autonome en la matière, l'intégralité de l'architecture informatique étant hébergée dans notre Datacenter sécurisé localisé **en France** (Clermont-Ferrand).

Les orientations stratégiques en matière de sûreté sont :

- Protéger l'ensemble des collaborateurs des Entités dans le cadre de leur mission ;
- Protéger les installations physiques et en particulier les Datacenters ;
- Protéger l'ensemble des systèmes d'information ;
- Préserver et protéger le patrimoine informationnel ainsi que les données qui lui sont confiées ;
- Protéger le savoir-faire ;
- Protéger les projets ;
- Veiller à l'intégrité, la réputation et la notoriété des Entités du Groupe.

Pour permettre au **Groupe** d'atteindre ses objectifs de sûreté, les règles de sécurité sont fixées dans une Directive de Sécurité de l'Information Générale (DSIG). La présente Directive s'applique dans toutes les Entités **à tous les collaborateurs**, employés ou prestataires, **ayant un accès aux systèmes d'information du Groupe**.

Les règles décrites dans cette Directive sont établies par le RSSI et validées par le Représentant de l'établissement français de BE INVEST International SA. Leur mise en application reste sous la responsabilité de l'Entité qui doit les appliquer et peut les compléter, si besoin, par sa propre politique de sécurité.

Le **Prestataire** dispose de sa propre Politique de Sécurité de l'Information (PSI) qui s'appuie sur la PSIG et DSIG BeYs.

Présentation du plan de Continuité d'Activité dans l'annexe **Plan de Continuité d'Activité**.

Notre site de Clermont-Ferrand est :

- Sous vidéosurveillance ;
- Sous télésurveillance ;
- Soumis à un contrôle d'accès par badge sans contact ;
- Soumis à un contrôle d'accès biométrique pour les zones sensibles.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation



Figure 2 : Bâtiment et Data Centers, situé à Clermont-Ferrand

Le Datacenter, nommé « LA CITADELLE DATACENTER », est composé de deux datacenters distincts hébergés sur la même emprise géographique sur le site de Clermont-Ferrand. Il est construit suivant un concept de poupées russes au niveau de l'infrastructure physique, des réseaux, du matériel, des applications, des données et des accès. À chaque niveau de sensibilité de l'information correspond une nouvelle poupée russe.

Une description plus détaillée de nos locaux, de nos datacenters et de nos politiques et procédures de sécurité sont présents dans différents documents qui sont **consultables uniquement sur site**.

Nous retrouvons ainsi pour le premier datacenter, nommé DC1 :

- Une première poupée russe correspondant à l'emprise du bâtiment ;
- Une seconde poupée russe correspondant aux zones techniques du Datacenter ;
- Une troisième poupée russe correspondant au premier environnement, salle informatique, nommé environnement 1, pour des traitements « classiques », anciennement nommé salle machine ;
- Une quatrième poupée russe correspondant au second environnement, salle informatique, nommé environnement 2, pour des traitements « sécurisés », anciennement nommé salle bunker.

Pour le second datacenter, nommé DC2, nous retrouvons :

- Une première poupée russe correspondant à l'emprise du bâtiment ;
- Une seconde poupée russe correspondant aux zones techniques du Datacenter ;
- Une troisième poupée russe correspondant au troisième environnement, salle informatique, nommé environnement 3, pour des traitements « sensibles », anciennement nommé salle machine ;

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

- Une quatrième poupée russe correspondant au quatrième environnement, salle informatique, nommé environnement 4, pour les traitements de confiance numérique et les traitements et stockages de données sensibles », anciennement nommé salle bunker ;
- Une cinquième et sixième poupée russe au niveau du double sarcophage entourant deux cages de Faraday, nommés environnement 5a et 5b.

À chaque nouvelle poupée russe des éléments d'authentification supplémentaires sont ajoutés pour les accès physiques, ainsi que des cloisonnements supplémentaires au niveau de la sécurité du SI.

À titre d'information, le contrôle d'accès physique mis en place au niveau du Datacenter correspond au niveau le plus élevé des recommandations des technologies sans contact publié par l'ANSSI, et les surqualifie aux niveaux de traitement les plus sensibles de l'information.

En complément la détection d'intrusion est vue en profondeur, depuis l'emprise externe du site vers les zones de sensibilités les plus fortes, en associant des mesures passives et actives, des technologies différentes (sas unipersonnel, clôtures détectrices, câbles choc, caméras thermiques, lasers, etc.).

Pour de plus amples informations sur la sécurité que nous mettons en place sur nos différents produits, vous pouvez vous référer à notre Plan d'Assurance Sécurité (PAS).

10.2 Sécurité physique, bâtementaire et électronique

Le site de Clermont-Ferrand où sont positionnés deux ensembles de datacenters hautement sécurisés (dont l'un est en accès réglementé par l'Etat Français), est un site hautement protégé, gardienné 7/7, 24/24.

Dans le domaine de la sécurité bâtementaire, sur l'emprise géographique de Clermont-Ferrand sont positionnées trois systèmes de gestion centralisée des bâtiments ou GTB.

Supervisés 24H/24, 7/7 ces systèmes, intégrant les aspects de cybersécurité, sont déployés :

- Au niveau des bâtiments de type tertiaire,
- Au niveau du premier Datacenter DC1,
- Au niveau du second Datacenter DC2.

Un bureau sécurité est en place. Il est piloté par le Responsable Sûreté Entreprise, en charge de la vidéosurveillance. Nous exerçons un contrôle régulier des caméras et nos enregistrements sont conservés durant 30 jours. Ils sont stockés dans un local sécurisé sous double authentification avec détection d'intrusion, cloisons renforcées et protection contre la poussière.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Nos agents de sécurité, équipés de moyens de communication, effectuent des patrouilles à l'extérieur du bâtiment selon un planning confidentiel. Toutes les issues donnant sur l'extérieur ferment à clé et les fenêtres du rez-de-chaussée sont munies de verres spécifiques contre l'effraction et l'intrusion.

Des systèmes de détection d'intrusion ont été installés au niveau du bâtiment. Ces systèmes sont reliés à une télésurveillance 24h/24 respectant les règles APSAD. Les centrales d'alarme, parties intégrantes du système de sécurité, sont installées dans des locaux hautement sécurisés, protégés par un contrôle d'accès et des murs renforcés. L'accès à ces locaux n'est autorisé qu'au seul personnel habilité.

Les centrales d'alarme disposent de batterie assurant l'autonomie du système sur 72 heures. Le cœur du système de sécurité regroupe les enregistreurs numériques, les serveurs des systèmes et les centrales d'alarme.

10.2.1 La sécurité physique de notre infrastructure

Le système de protection de toute information ou support protégé est constitué de plusieurs « barrières » cohérentes, inclusives et successives : l'emprise du bâtiment et/ou le bâtiment lui-même, le local qui contient le meuble, le meuble dans lequel est conservée l'information ou le support protégé.

Les barrières sont classées suivant des mesures de protection de deux types : actives et passives.

Le site contenant le datacenter LA CITADELLE DATACENTER est :

- Sous vidéosurveillance, système ayant fait l'objet d'une déclaration auprès de la CNIL ;
- Sous télésurveillance, via un prestataire de confiance externe ;
- Soumis à un contrôle d'accès par badge sans contact ayant fait l'objet d'une déclaration auprès de la CNIL ;
- Soumis à un contrôle d'accès biométrique pour les zones sensibles ayant fait l'objet d'une demande d'autorisation auprès de la CNIL.

Le site de Clermont-Ferrand où sont positionnés deux ensembles de Datacenters hautement sécurisés (dont l'un est en accès réglementé par l'Etat Français), est un site hautement protégé, gardienné 7/7, 24/24.

Pour l'accès à nos datacenters, l'autorisation d'accès est soumise à contrôle dans le cadre de la Protection du Potentiel Scientifique et Technique de la nation (PPST). De ce fait, tout personnel, y compris les auditeurs, devant accéder physiquement au datacenter ou logiquement aux systèmes d'exploitation ou à l'infrastructure réseau hébergés doit obtenir un avis favorable du Haut Fonctionnaire de Défense et de Sécurité (HFDS).

Du fait du haut niveau de sécurité, de la sensibilité des informations hébergées et de la PPST, seule une visite sur site permettra au(x) auditeur(s) de faire tous les

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

constats de sécurité et d'implantation mis en place. Aucune visite virtuelle n'est possible.

L'attribution de ces accès se fait selon une **procédure de gestion des accès physiques** liée au « besoin d'en connaître », c'est-à-dire de ne fournir des autorisations ou habilitations qu'aux personnes dont la fonction nécessite ces droits. La règle de base est que l'accès n'est valide que le temps nécessaire lié au strict « besoin d'en connaître ».

Au niveau du bâtiment, certains bureaux ainsi que les salles informatiques ne peuvent être accessibles que pour des personnels nommément identifiés. Ces accès sont alors garantis par un contrôle associé à des profils spécifiques.

Les zones sensibles du site bénéficient d'un système de sécurité renforcé. Tout personnel non habilité n'accède aux zones sensibles qu'en présence et sous contrôle des agents de sécurité (cas du ménage par exemple).

Les salles de DC1 et DC2 disposent des systèmes de sécurité physique suivants :

- Un système de secours électrique en capacité de pallier un défaut d'approvisionnement du réseau sans interruption d'approvisionnement électrique. Le secours électrique doit s'appliquer aussi aux systèmes de sécurité et systèmes de refroidissement ;
- Un système de secours du système de refroidissement principal ou un système préventif permettant de préserver les actifs en cas de défaut ;
- Un système de détection d'incendie ainsi qu'un système d'extinction conçu de manière à ne pas détruire le matériel en cas de déclenchement ;
- Un système de contrôle d'accès physique et de détection d'intrusion permettant de limiter l'accès au personnel nominativement habilité et de tracer les visites ;
- Un système de secours des télécommunications ;
- Un système de détection de présence de fluide.

L'ensemble des systèmes assurant la sécurité et la continuité dans nos datacenters a été conçu et implémenté avec des redondances systématiques que ce soit au niveau électrique, climatisation, réseaux, ...

Le niveau global de sécurité des datacenters est conforme au niveau le plus élevé du guide de l'Agence nationale de la sécurité des systèmes d'information (l'ANSSI) sur les technologies sans contact et en conformité avec la norme APSAD D83. Des systèmes de détection d'intrusion ont été installés au niveau du bâtiment. Ces systèmes sont reliés à une télésurveillance 24h/24 respectant les règles APSAD. Les centrales d'alarme, parties intégrantes du système de sécurité, sont installées dans des locaux hautement sécurisés, protégés par un contrôle d'accès et des murs renforcés. L'accès à ces locaux n'est autorisé qu'au seul personnel habilité.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

L'ensemble des équipements assurant la protection des salles informatiques est maintenu régulièrement. Un suivi de la maintenance est effectué, formalisé dans un fichier Excel (planning de maintenance) et contrôlé.

Les systèmes de sécurité physiques sont implémentés sur un réseau physiquement indépendant du SI et non connecté à l'Internet. Cela garanti la protection contre toute attaque sur les systèmes de sécurité.

Les salles informatiques sont équipées de systèmes de détection et de protection permettant de réduire le risque de désastre potentiel (feu, inondation...), pilotés par un système de Gestions Techniques Centralisés (GTC) regroupant :

- Des mécanismes de détection et d'extinction de feu ;
- Des mécanismes de détection d'inondation ;
- De la surveillance de température et d'humidité (hygrométrie) ;
- Un système de climatisation ;
- Des redondances des alimentations et garanties du secours.

Des alertes sont envoyées par SMS à la sécurité et au gestionnaire technique par le système GTC.

La protection incendie du bâtiment repose sur un ensemble de détecteurs reliés à un Système de Détection Incendie (SDI).

Le système d'extinction d'incendie assure une protection maximum contre toute dégradation du matériel informatique dans les datacenters : utilisation de buses spécifiques pour l'éjection du gaz d'extinction (pas de sprinklers) permettant d'éviter un phénomène de résonance avec les disques mécaniques du système d'information.

L'emprise du bâtiment situé au niveau altitude zéro par rapport au fil d'eau dispose de sondes d'inondation reliées à un système de GTB (Gestion Technique de Bâtiment). Ces sondes de détection d'humidité sont positionnées dans les datacenters afin de protéger toute dégradation du système d'information par un fluide.

10.3 La sécurité de notre Système d'Information

Nous avons mis en œuvre des infrastructures IT hautement sécurisées, permettant l'hébergement sécurisé d'applications, ou plus généralement d'environnements informatiques :

- Hébergement dans un Datacenter hautement sécurisé au niveau physique, disposant notamment d'une zone bunker et de cages de Faraday, réservés à l'hébergement de données ou de fonctions extrêmement sensibles (ex : services cryptographiques) ;
- Réseaux et infrastructure IT mettant en œuvre le principe de défense en profondeur, en particulier via plusieurs zones de confiance aux points

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

d'interconnexion filtrés et contrôlés (firewalls, reverse-proxies, etc.) et équipés de dispositifs de détection d'intrusion (IDS/IPS) ;

- Surveillance et traitement des vulnérabilités et des événements de sécurité issus de l'infrastructure et des dispositifs de détection, par un SOC interne ;
- Veille continue des menaces, réalisée par une cellule cybersécurité.

La sécurité du SI (ou sécurité informatique) est pilotée par le Responsable Sécurité des Systèmes d'Information (RSSI) de BE INVEST International SA et l'équipe SOC de cybersécurité de be ys cloud France, et a en charge plusieurs missions couvrant le cycle de vie complet des menaces et des composants du SI.

10.4 Antivirus centralisé et patch de sécurité

Les Entités BeYs disposent d'un moteur antivirus centralisé protégeant la totalité des serveurs Windows et son parc micro-informatique. En plus de la fonction d'antivirus, la solution comporte des fonctions étendues de protection des navigateurs et de pare-feu système (Solution de type Endpoint). Un contrat de maintenance est souscrit pour ces anti-virus par be ys cloud France. Les moteurs et les fichiers de signatures sont tenus à jour.

En ce qui concerne les serveurs IBMi, un contrat d'assistance logicielle est souscrit avec l'éditeur. Dans le cadre de ce contrat, l'éditeur met à disposition les mises à jour d'Operating System (OS) et les patchs de sécurité qui sont appliqués à fréquence régulière (a minima 1 fois /an en fonction de leur disponibilité). Les patchs de sécurité les plus critiques sont appliqués dès leur mise à disposition.

Pour les serveurs, chaque « propriétaire » de serveur tient la mise à jour des correctifs de sécurité en fonction des informations de vulnérabilités remontées par le SOC.

Pour les postes de travail, BE INVEST International SA assure le patch management du parc micro-informatique et tient à jour le dernier niveau de correctifs de sécurité.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

10.5 Intrusions

Notre SAE utilise des éléments de sécurité comme des **pares-feux** (firewall), des locaux télécoms, différentes salles informatiques jusqu'à un cœur cryptographique. La haute disponibilité de ces équipements est assurée en mode cluster, via des interfaces et VLAN dédiés, répartie en salles de production informatique primaire (DC2) et secondaire (DC1).

Nos équipements portant les fonctions d'**offloading et onloading SSL** et de **pare-feu applicatif** (WebApplication Firewalling) prennent place dans une « zone démilitarisée » (DMZ) entre 2 rangées de Firewalls en entrée/sortie des environnements 1 et 2 ou 3 et 4. La haute disponibilité de ces équipements est assurée en mode cluster, via des interfaces et VLAN dédiés, réparti en salles de production informatique primaire et secondaire.

Nos équipements portant les fonctions de **reverse-proxy** et **répartiteurs de charge** (load balancer) sont situés au plus près des serveurs placés dans les zones suivantes : les salles machine et les bunkers. La haute disponibilité de ces équipements est assurée en mode cluster, via des interfaces et VLAN dédiés, réparti en salles de production informatique primaire et secondaire.

10.6 Sécurisation des échanges

La sécurité commence par les échanges. Pour cela et afin de sécuriser au maximum les flux entre le client et notre SAE **ArchiveMi**, nous utilisons un tunnel VPN entre les deux systèmes d'informations. Les flux de navigation Web sur la plateforme s'effectuent au travers du tunnel VPN, couplé à un chiffrement HTTPS standard, cependant, lors des ateliers techno-fonctionnels, le Prestataire peut s'adapter aux contextes du Client

10.7 Protection des données personnelles

Eu égard aux enjeux spécifiques des données personnelles hébergées, le **Prestataire** dispose d'un DPO (Data Protection Officer). Celui-ci a construit une organisation autour de la protection des données à caractère personnel impliquant différents acteurs en interne dont

- Le Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- La Directrice Juridique ;
- Ainsi que le SOC.

Le respect de la Loi Informatique et Liberté, ainsi que le RGPD, est positionné comme élément central de l'activité du Groupe. Une fiche réflexe sur la protection des données à caractère personnel permet à tout Chef de Projet d'intégrer au plus tôt cette problématique.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

10.8 Conformité réglementaire et juridique

Pour répondre aux différentes exigences légales et réglementaires, le **Prestataire** dispose via BE INVEST International SA d'une cellule de conformité juridique.

Elle est composée d'experts sur les réglementations légales en termes de traitement de données et d'hébergement de données de santé (référentiel HDS de l'ASIP-Santé) et d'une juriste compétente en cybersécurité, qui assurent la veille et le conseil nécessaires au maintien de nos référentiels de conformité.

10.9 Réplication des archives

Les documents archivés sont immédiatement répliqués sur un site distant (réplication en « Y ») afin de redonder les documents archivés comme l'exige la norme NF Z42-013. Notre service d'archivage dispose donc d'une architecture sur 2 sites (référence à la norme NF Z42-013). Ces deux sites correspondent aux deux bâtiments situés 46 rue du Ressort à Clermont-Ferrand.

Nous avons également un troisième site, situés 60 Avenue Rockefeller, 69008 Lyon, qui est utilisé uniquement pour l'externalisation du stockage des sauvegardes.

Pour obtenir de plus amples informations sur notre réplication en « Y » des documents, vous pouvez vous référer à notre dossier de description technique du système (DGTS).

10.10 Horodatage

L'horodatage est un mécanisme qui consiste à associer une date et une heure à un événement, une information ou une donnée informatique. Il a pour but d'enregistrer l'instant auquel une opération a été effectuée. Il se traduit habituellement sous la forme d'une séquence de caractères représentant la date et l'heure à laquelle est survenu un événement, associée à un texte décrivant ledit événement. La date et l'heure sont généralement représentées de façon à faciliter la comparaison entre événements, ce qui permet de suivre le déroulement d'un ensemble d'opération de manière relativement aisée. La norme internationale ISO 8601 spécifie une représentation de la date et de l'heure universelle.

Notre horodatage s'appuie donc sur une synchronisation des serveurs par le protocole NTP. Les traces (contenant l'horodatage) sont stockées dans les journaux.

10.11 Continuité de service

L'objectif du Prestataire est de garantir la **disponibilité**, l'**intégrité**, la **confidentialité** et la **qualité** des fonctions et des informations sensibles pour l'ensemble de nos prestations, de nos offres de services et de nos processus internes. Une attention particulière est apportée à la gestion des données sensibles (données administratives, données financières, données de santé, données à caractère personnel).

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Le Prestataire dispose d'un PCA/PRA afin d'assurer une mise en œuvre des mesures raisonnables afin de veiller à la continuité et à la reprise des activités informatiques vis-à-vis de la prestation fournie.

Le **Prestataire** contrôle et surveille la cohérence des AIP conformément à sa procédure en vigueur de contrôle et surveillance de la conservation. En cas de perte ou de corruption des documents numériques et/ou des métadonnées, le Prestataire préviendra le Client associé et restaurera dans les délais et modalités convenus dans le contrat, les éléments perdus ou corrompus. Une fois les données restaurées, le Prestataire contrôlera à nouveau la cohérence des éléments restaurés et notifiera le Client associé de sa résolution.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

Afin de garantir un service de qualité, le Prestataire suit un certain niveau de service via les indicateurs suivants :

- Niveau de disponibilité ;
- Un RTO de 4 heures ;
- Un RPO de 0 car l'objectif d'un système d'archivage et de ne perdre aucun document, aucune métadonnée ou élément de preuve attestant de la bonne conformité des informations présentes dans le SAE.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés **be ys trusted solutions France** - Toute reproduction ou diffusion même partielle interdite sans autorisation

11 *PRINCIPE* *S TECHNIQUES DE LA RÉVERSIBILITÉ*

11.1 Principe

La réversibilité peut notamment être motivée par plusieurs facteurs, tels que :

- L'arrêt de la prestation du service d'archives d'origine, par exemple en cas d'arrêt d'un contrat de tiers archivage pour les fonds concernés ou cessation d'activité ;
- Le transfert vers un autre SAE, après une période de conservation dans le SAE d'origine (par exemple un système d'archivage définitif).

Cette procédure permet d'assurer la pérennité d'une archive sans en compromettre son intégrité.

11.2 Mode opératoire

Conformément à notre annexe de réversibilité, le Client doit formuler par écrit sa demande en fin de contrat ou en cas de résiliation anticipée. Pour de plus amples informations, merci de vous référer au document sus-évoquée « Plan de réversibilité ».

Si le Client souhaite un export dans un format spécifique que celui proposé par défaut par le Prestataire, alors les parties devront se rencontrer pour déterminer la faisabilité et le coût afférent.

Dès réception de la demande de réversibilité et une fois le dernier jour d'usage atteint, le Prestataire :

- Empêche tout versement et élimination des archives tout en gardant la consultation des archives opérationnelle
- S'engage, selon les modalités prévues au contrat, à restituer les archives, les métadonnées associées, la signature de l'empreinte des différentes archives et les différentes traces générées par les archives durant le cycle de vie via un canal ou support sécurisé tel que :
 - o Mise en place d'un coffre-fort électronique ;
 - o Transfert SFTP (SSH File Transfer Protocol) qui se traduit par un transfert de fichiers sécurisé par SSH ;
- Remise en main propre d'un disque dur chiffré (pouvant générer des coûts supplémentaires).
- Ferme le SAE ArchiveMi et toutes les connexions liées au Client (compte d'accès et/ou VPN) seront supprimées

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation

A l'issue de ce transfert, le Client transmet au Prestataire un procès-verbal de fin de réversibilité afin de valider les opérations, ou émet des réserves. Ce procès-verbal peut être transmis soit par courriel ; soit courrier postal. Le procès-verbal définitif sans réserve marque le transfert de responsabilité entre le Prestataire et le Client ou le tiers habilité par celui-ci. En cas de réserves émises par le Client, le Prestataire dispose d'un délai complémentaire pour y remédier.

A défaut de procès-verbal et selon les modalités prévues dans notre plan de réversibilité, le Prestataire relancera le Client par courriel ou courrier postal. Sans réponse du Client et selon les modalités de notre plan de réversibilité, le Prestataire pourra procéder à la suppression définitive de toutes les données du Client, la restitution totale étant réputée valide par défaut.

Le Prestataire s'engage à l'issue de la phase de réversibilité et après acceptation des procès-verbaux définitifs par le Client, à supprimer l'ensemble des données de ce dernier et à ne conserver aucune copie (données, informations ou documents).

Les opérations de destruction des données font l'objet d'un procès-verbal de destruction transmis par courriel ou courrier postal au Client.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés **be ys trusted solutions France** - Toute reproduction ou diffusion même partielle interdite sans autorisation

12 FONCTIONNEMENT DU SERVICE

FONCTIO

12.1 Auditabilité

Le SAE ArchiveMi est conçu et exploité par notre société qui s'appuie sur un hébergement qui dispose des certifications ISO 27001 et HDS sur le périmètre de l'hébergement physique des données détenues par notre sous-traitant **be ys cloud France**.

Le client a la possibilité d'organiser ses propres audits sur notre SAE ArchiveMi afin de suivre et de contrôler tout le cycle de vie des documents électroniques archivés selon les conditions prévues au Contrat.

12.2 Niveau de service

Le service d'archivage est rendu selon un niveau de Qualité prévu au Plan de Qualité de Service. Ce document annexé au contrat prévoit en particulier, les conditions de suivi de la qualité, les procédures de déclaration d'incident et les délais de prise en compte et/ou correction ainsi que le taux de disponibilité et les éventuels indicateurs de performance.

Public

be ys trusted solutions France

10 boulevard Haussmann, 75009 PARIS

© Tous droits réservés be ys trusted solutions France - Toute reproduction ou diffusion même partielle interdite sans autorisation