

Informations sur le Service Silae Paie Cloud Azure

Août 2023

Sommaire

1. Objet	3
2. Définitions	3
3. PérimÈtre du service	4
4. AccÈs au Service	5
5. Maintenance	5
6. Disponibilité du Service	6
7. Infrastructure d'hÉbergement Microsoft Azure	7
7.1. Conformité et Certifications de la plateforme Microsoft Azure.....	7
7.2. Sécurité de la plateforme Microsoft Azure	8
7.2.1. Sécurité des Réseaux.....	8
7.2.2. Sécurité des Stockages	9
7.2.3. Sécurité des Bases de Données	9
7.3. Localisation de l'exploitation.....	10
7.4. Continuité de l'exploitation	10
8. Administration et Supervision du Service	11
9. Gestion des Sauvegardes et des Restaurations	11
9.1. Sauvegarde des Bases de Données.....	12
9.2. Restauration des Bases de Données.....	12
9.3. Sauvegarde des Fichiers	14
9.4. Restauration des Fichiers	15
10. Mise à Jour.....	15

1. OBJET

Ce document a pour objet d'informer le Partenaire et le Client sur la nature de l'ensemble des prestations souscrites auprès de Microsoft Azure et liées à l'hébergement, la qualité de service, la maintenance et la sécurité de l'application Silae (le Service) délivrée en mode SaaS et hébergée dans le Cloud.

2. DÉFINITIONS

« Cloud » (ou cloud computing) : en français « informatique en nuage », correspond à la fourniture de services informatiques (serveurs, stockage, bases de données, réseaux, etc.) à distance via Internet et un fournisseur spécialisé. Le principal service logiciel proposé en cloud computing est le SaaS.

« SaaS » (Software as a Service) Logiciel en tant que Service est un modèle de distribution de logiciel à travers le Cloud. L'hébergement des applications est sous la responsabilité du fournisseur du Service. La solution SaaS est accessible à la demande via une connexion Internet. La mise à disposition, la maintenance évolutive et corrective, les mises à jour sont de la responsabilité de l'éditeur du logiciel SaaS.

« Client » désigne toute société utilisatrice des services SILAE et souhaitant un accès à la plateforme pour ses collaborateurs.

« Période de Maintenance » désigne une période durant laquelle le Service peut être interrompu pour effectuer des maintenances applicatives et techniques conformément aux dispositions du présent document.

« Heures ouvrées » désigne les heures d'ouverture du service d'assistance Silae.

« Mises à Jour » désigne les améliorations apportées au Service (logiciel Silae et infrastructures informatiques sous-jacentes). Les Mises à Jour comprennent également la correction d'éventuelles anomalies et les améliorations fonctionnelles ou légales liées au domaine de la Paie.

« API » (Application Programming Interface), en français « interface de programmation d'application », désigne l'ensemble des définitions et des protocoles qui facilitent l'intégration du Service avec d'autres applications.

« Incident Critique » désigne un incident entraînant une interruption totale et non programmée du Service.

« Microsoft Azure » désigne la plate-forme Microsoft Azure et correspond aux offres d'informatique en nuage public de type PaaS et IaaS de Microsoft.

« ISO » (International Organisation for Standardization) ou Organisation Internationale de Normalisation est une organisation ayant pour but de produire des normes internationales dans les domaines industriels et commerciaux.

« Cloud Security Alliance (CSA) » est la principale organisation mondiale qui se consacre à la définition et à la sensibilisation des meilleures pratiques afin de garantir un environnement informatique en nuage sécurisé.

« Cloud Controls Matrix (CCM) » est un cadre de contrôle de la cybersécurité pour l'informatique en nuage piloté par la Cloud Security Alliance.

« CSA STAR Certification » désigne un label de sécurité pour le Cloud. Les Certifications de la « Cloud Security Alliance » s'appuient sur les certifications ISO 27001 et la Cloud Control Matrix.

3. PÉRIMÈTRE DU SERVICE

Le périmètre effectif du Service est l'application Silae Paie.

Le Service inclut l'application de gestion de la paie et toutes les fonctionnalités associées permettant aux Partenaires d'opérer toutes les tâches de gestion de la paie disponibles dans le logiciel ou les APIs associées.

4. ACCÈS AU SERVICE

Le Service est délivré en mode SaaS et nécessite une connexion Internet.

Silae n'est pas responsable de la qualité de la connexion Internet utilisée pour accéder au Service.

Les modalités d'accès au Service (adresse internet d'accès ou URL) sont transmises lors de la création du compte.

Par défaut, le Service est ouvert tous les jours, 24h sur 24h.

Il peut cependant être interrompu durant les Périodes de Maintenance ou lors de Maintenance Urgentes. L'ensemble des Maintenance possibles est listé dans la section Maintenance du présent document.

5. MAINTENANCE

Le Service peut être interrompu durant les Périodes de Maintenance et pour de la Maintenance Urgente.

Périodes de Maintenance :

- Maintenance Standard
Toutes les nuits entre 2h00 et 4h00 (Central European Time CET/ Central European Summer Time CEST).

La période de Maintenance Standard permet d'assurer la mise à jour du Service (logiciel et infrastructures) pour garantir la qualité de service. Le Service peut éventuellement rester accessible pendant la Période de Maintenance car la probabilité de couper l'accès aux Services sur l'intégralité de la Période de Maintenance reste faible.

- Maintenance Exceptionnelle et Planifiée

Une Maintenance Exceptionnelle et Planifiée peut être opérée en dehors des périodes de Maintenance Standard. Silae a l'obligation de communiquer sur cette intervention au moins 48 heures avant l'heure prévue de ladite maintenance.

- Maintenance Urgente

Une Maintenance Urgente est susceptible d'intervenir à tout moment. Cette maintenance peut intervenir en cas de force majeure et Silae s'engage à mettre en œuvre tous les moyens possibles pour tenir informé les Partenaires et les Clients sur l'évolution des opérations liées à cette maintenance.

6. DISPONIBILITÉ DU SERVICE

Silae s'engage à fournir un Taux de Disponibilité (TD) mensuel du Service d'au moins 99,5%.

Le taux de disponibilité (TD) est défini comme la possibilité de se connecter au Service dans la période de référence (PR).

La période de référence (PR) correspond aux temps en dehors des Périodes de Maintenance effectives (de tout type).

Le temps d'indisponibilité (TI) du service n'est calculé qu'en dehors des Périodes de Maintenance effectives (et de tout type) et lorsque le Service est totalement inaccessible (Incident Critique.)

Formule de calcul : $TD = (PR - TI) / PR$

TD : taux de disponibilité

PR : période de référence

TI : temps d'indisponibilité

Les incidents entraînant des problèmes d'accès au Service et ne révélant pas du contrôle de Silae ne peuvent, en aucune manière, être considérés comme du Temps d'Indisponibilité.

Incidents non éligibles :

- Difficultés d'accès au Service dues à une mauvaise configuration du poste de travail du Client.
- Problèmes de télécommunication (accès internet et réseau d'entreprise) chez le Client ou chez le fournisseur d'accès du Client.
- Défaut dans le système informatique du Client.
- Tout autre incident, hors de contrôle de Silae, interdisant le fonctionnement optimal du Service pour le Client.
- Un incident lié à un fournisseur critique et hors de contrôle de Silae.

7. INFRASTRUCTURE D'HÉBERGEMENT MICROSOFT AZURE

Le Service Silae est délivré via un environnement sécurisé, assurant le contrôle des accès, la continuité de service, le stockage et la protection des données, l'exploitation des équipements et la connectivité aux réseaux distants.

Les infrastructures Silae liées au Service sont hébergées sur la plateforme Microsoft Azure.

Microsoft Azure est considéré par Silae comme un fournisseur critique.

Liste non exhaustive des services de la plateforme Microsoft Azure opérés par Silae pour la délivrance du Service :

- Les services de type Compute (Calcul) :
 - Azure Virtual Machines, Azure Virtual Machines ScaleSet, Azure Compute Gallery, Azure App Service.
- Les services de Stockage :
 - Azure Blob Storage, Azure File, Azure Recovery Service, Azure Shared Image Gallery
- Les services de Bases de Données :
 - Serveurs Azure Database pour MySQL
- Les services de réseau et sécurité réseau :
 - Azure DNS, réseaux virtuels, pare-feu, groupes de sécurité réseau, bastion, Azure Application Gateway
- Les services de sécurité :
 - Azure Active Directory, Azure Active Directory Domain Service, Azure KeyVault
- Les services de supervision d'infrastructure intégrés :
 - Azure Monitor et Azure Application Insight

7.1. Conformité et Certifications de la plateforme Microsoft Azure

La plateforme Microsoft Azure dispose de nombreuses certifications ISO (International Organization for Standardization) et CSA (Cloud Security Alliance) et propose une couverture de conformité réglementaire très large.

L'ensemble de la documentation liée à la conformité Azure est disponible ici :
<https://docs.microsoft.com/fr-FR/azure/compliance/>

Les certifications CSA STAR sont disponibles ici :

<https://cloudsecurityalliance.org/star/registry/microsoft/>

Les rapports d'audit et les certifications associées sont disponibles ici :
<https://servicetrust.microsoft.com/Documents/ComplianceReports>

7.2. Sécurité de la plateforme Microsoft Azure

Dans le cadre de son exploitation, Silae s'appuie sur l'expérience et sur l'expertise de Microsoft et des services proposés par la plateforme Microsoft Azure.

La plateforme Azure offre de nombreux mécanismes pour effectuer la sécurisation, la gestion et la surveillance des services et des équipements. La sécurité du Service Silae hérite implicitement d'un nombre important de fonctionnalités Azure liées à la sécurité.

L'ensemble de la Sécurité du Service Silae repose sur une responsabilité partagée. Microsoft est responsable de la gestion de ces centres de données et de l'ensemble du périmètre de sécurité associé (intégrité physique des bâtiments et des équipements, protocoles d'accès, protections incendie, etc.). Azure fournit aussi un ensemble de services logiciels liés à la sécurité qui répond aux exigences de Silae.

Une présentation de la stratégie de sécurité Microsoft Azure est disponible ici :
<https://docs.microsoft.com/fr-fr/azure/security/fundamentals/overview>

Microsoft met en œuvre les meilleures pratiques de sécurité existantes sur l'ensemble de ses services pour garantir la disponibilité, l'intégrité et la confidentialité des données. Silae se conforme à ces bonnes pratiques pour assurer l'exploitation et la sécurité du Service.

7.2.1. Sécurité des Réseaux

Silae met en œuvre des services Azure pour la conception de son architecture réseau en respectant un cloisonnement et un strict contrôle des accès.

Ces architectures s'appuient notamment sur la séparation des réseaux et l'usage des sous-réseaux (subnetting), sur le réseau virtuel Azure et la mise en place de DMZ.

Les ressources de production Azure sont totalement isolées du reste du Système d'Information Silae d'un point de vue des flux réseau et droits d'accès au sein de leurs groupes de ressources.

La sécurisation des accès est assurée par les services suivants (propres à chaque groupe de ressources ou de sous-réseaux au sein d'un groupe de ressources) :

- Le service de sécurité réseau Pare feu Azure avec des groupes de sécurité réseau interdisant les flux externes inutiles et n'autorisant pour les actions de gestion que les protocoles autorisés aux exploitants depuis les réseaux internes de Silae.

- Le service de passerelle « Azure Bastion » limite la connexion aux ressources à ces exploitants en interdisant notamment le protocole RDP sur Internet.
- Le service « Azure Application Gateway » pour sécuriser les accès HTTPS.
- Les services de sécurité suivants sont utilisés pour la sécurisation des accès : Azure Active Directory, Azure Active Directory Domain Service, Azure KeyVault.

Le contrôle de l'accès aux différents composants du réseau est assuré par la mise en place de NSG (Network Security Group.)

La surveillance des réseaux, des flux et du trafic est assurée via les services suivants :

- Azure Monitor
- Azure Network Watcher

7.2.2. Sécurité des Stockages

Les données entreposées sur les stockages Azure sont systématiquement chiffrées au repos. Le chiffrement s'applique également aux disques des serveurs managés.

Les services exploités sont configurés pour utiliser les services de chiffrement de la façon suivante :

- Les disques des machines virtuelles (VMs, groupes de VMs ou AppService) sont des Disques Gérés (Managed Disks) avec chiffrement au repos SSE de type PMK.
- Les services de stockage ne sont accessibles que sur le réseau virtuel interne de chaque groupe de ressources et via des protocoles sécurisés : TLS 1.2, ou SMB avec sécurisation Azure Managed Identities.
- Référence : chiffrement côté serveur de disques managés Azure - Azure Virtual Machines | Microsoft Docs
<https://docs.microsoft.com/fr-fr/azure/virtual-machines/disk-encryption>

7.2.3. Sécurité des Bases de Données

Les bases de données sont systématiquement chiffrées au repos. Les mécanismes de Chiffrement transparent des données (TDE, Transparent Data Encryption) assurent le chiffrement et le déchiffrement des données et des journaux en temps réel via une clé de chiffrement symétrique.

Les services exploités sont configurés pour utiliser les services de chiffrement au repos de la façon suivante :

- Les disques des serveurs Azure Database pour MySQL, les sauvegardes de bases de données et les fichiers temporaires sont encryptés via le protocole FIPS 140-2 et l'algorithme AES 256 bits.
- Les bases de données sont accessibles uniquement localement (réseau virtuel) et via un protocole sécurisé par TLS 1.2
- Chaque instance PaaS de Azure Database pour MySQL dispose de sa propre clé de chiffrement.

- Les clés de chiffrement sont stockées dans un coffre-fort numérique à accès restrictif.
- Référence : Security - Azure Database for MySQL | Microsoft Docs
<https://docs.microsoft.com/en-us/azure/mysql/concepts-security>

7.3. Localisation de l'exploitation

Les infrastructures Azure (serveurs de calcul, serveurs de bases de données, stockages, services réseau, etc.), les données et les sauvegardes exploitées par Silae pour délivrer le Service sont exclusivement localisées sur le territoire métropolitain français. La zone Microsoft Azure « France Central » est la zone de référence pour l'intégralité de l'exploitation.

Les spécifications de cette zone sont consultables :

<https://azure.microsoft.com/fr-fr/regions/>

Silae se réserve le droit d'exploiter tous les centres de données Azure existants ou futurs liés à cette zone géographique.

La plateforme Microsoft Azure fournit une description détaillée des mécanismes d'accès aux données dans le document suivant :

<https://www.microsoft.com/fr-fr/trustcenter/privacy/who-can-access-your-data-and-on-what-terms>

7.4. Continuité de l'exploitation

La continuité de l'exploitation et la résilience des infrastructures s'appuient :

- Sur des solutions d'architecture et des mécanismes inhérents à la plateforme Microsoft Azure.
- Sur un ensemble des bonnes pratiques adoptées par Silae.

Les services Azure sont mis en œuvre pour garantir une disponibilité optimale dans toutes les situations de montée en charge. Les services et les infrastructures critiques sont systématiquement redondés.

Les solutions techniques Azure exploitées pour assurer la résilience reposent sur les solutions techniques suivantes (liste non exhaustive) :

- « Azure Load Balancer » pour l'équilibrage et la distribution de la charge réseau.
- « Azure Application Gateway » pour l'équilibrage de la charge applicative.
- « Azure for DataBase MySQL Flexible Server » pour les bases de données haute disponibilité.
- « Azure Virtual Machine ScaleSet » pour la montée en charge de la capacité de calcul (Compute).
- « Azure AvailabilitySet » ou « Availability Zone » pour la haute disponibilité géographique.

- « Azure File », « Azure Recovery Service », « Azure Shared Image Gallery » pour les stockages et les sauvegardes haute disponibilité.

Les engagements associés aux différents services Microsoft Azure (SLA) sont répertoriés dans le document suivant :

<https://azure.microsoft.com/fr-fr/support/legal/sla/>

Les spécificités de la continuité d'activité liées aux bases de données sont disponibles ici :

<https://docs.microsoft.com/fr-fr/azure/mysql/flexible-server/concepts-business-continuity>

8. ADMINISTRATION ET SUPERVISION DU SERVICE

L'administration et la supervision des architectures sont exclusivement réalisées par des opérateurs Silae.

Les services Azure sont supervisés par le service « Azure Monitor » : métriques de performance et des disponibilités, logs des actions de gestion/configuration sur les services, logs d'événements des services, alertes.

La disponibilité des Services applicatif Silae est supervisée par le service Azure Application Insight.

Les données de supervision sont conservées a minima un an pour assurer la bonne exploitation des services.

Pendant les Heures Ouvrées, la gestion des incidents est assurée par les opérateurs Silae en charge de l'exploitation.

En dehors des Heures Ouvrées, pendant les week-ends et les jours fériés, une équipe d'astreinte mise en place par Silae et opérant 24h/24h, assure la supervision et la résolution des incidents.

9. GESTION DES SAUVEGARDES ET DES RESTAURATIONS

Les sauvegardes et les restaurations sont essentielles de la stratégie de continuité d'activité de Silae, car elles protègent les données contre toute corruption ou suppression accidentelle.

Silae est responsable de la conduite des sauvegardes et des restaurations afin de sécuriser les données du Client.

9.1. Sauvegarde des Bases de Données

Silae s'appuie sur les mécanismes exposés par le service « Azure Database for MySQL Flexible Server ».

Des sauvegardes complètes (snapshots) des bases de données sont générées quotidiennement. Des sauvegardes des logs de transactions sont réalisées toutes les cinq minutes.

Les bases de données sont restaurables à partir de ces points de restauration sur un serveur MySQL provisionné sur demande.

Ces données et ces sauvegardes sont redondées plusieurs fois et uniquement au sein de la zone géographique définies dans la section « Localisation de l'exploitation ». Elles sont protégées contre les événements planifiés et non planifiés, notamment les défaillances matérielles transitoires, les pannes de réseau, les pannes électriques et les catastrophes naturelles.

Les sauvegardes des bases de données sont effectuées une fois par jour et avec une historisation de 35 jours.

Au-delà de cette période de 35 jours, Silae conserve une sauvegarde mensuelle pour les 12 derniers mois (la politique de rétention actuelle est mentionnée ici à titre indicatif et pourrait évoluer.) Cette sauvegarde mensuelle est déportée sur un compte de stockage de fichiers répondant aux exigences de sauvegarde des fichiers décrites plus bas dans cette annexe.

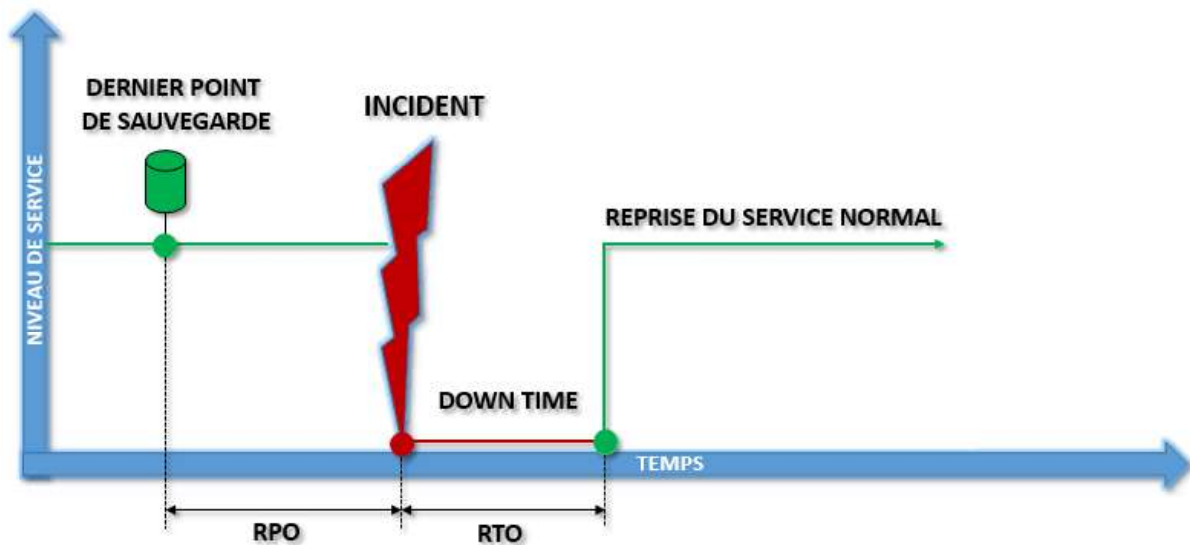
Les sauvegardes de base de données sont systématiquement chiffrées au repos avec des clés de chiffrement basées sur l'algorithme AES 256.

Les spécifications techniques sont disponibles ici :

<https://learn.microsoft.com/fr-fr/azure/mysql/flexible-server/concepts-backup-restore>

9.2. Restauration des Bases de Données

Silae s'engage à restaurer le Service sur la base de la sauvegarde la plus appropriée avec un RTO (Recovery Time Objective) maximum de 24 heures, et ce, dans les meilleurs délais.



Le RTO de 24h démarre à partir de la confirmation de la demande de restauration de la base de données. 24h00 est un temps maximum. Si une demande est réalisée le lundi à 9H00, la sauvegarde sera restaurée au plus tard mardi à 9h00. Cette fenêtre de temps est assez large car il est impossible de préjuger dans cette annexe de la taille de la base de données du Client. Silae dispose de sauvegardes clients qu'il est possible de restaurer en 15 minutes et d'autres avec 10 ans d'historique qui peuvent nécessiter plusieurs heures.

Le service est totalement inaccessible pendant toute la période de la restauration.

Le RPO minimal pour la restauration d'une base de données est d'une heure. En effet, Silae dispose de 35 jours d'historisation et de logs transactionnels qui permettent de cibler une heure donnée.

La perte de données maximale est donc d'une heure.

Le RPO peut être n'importe quelle heure sur les 35 derniers jours. Au-delà de ces 35 jours, Silae peut s'appuyer sur une des bases de données historisées chaque mois sur les 12 derniers mois.

9.3. Sauvegarde des Fichiers

En synthèse :

- Les fichiers supprimés sont conservés 365 jours (suppression réversible.)
- Nous sauvegardons tous les fichiers quotidiennement et conservons un historique de 14 jours.
- Nous assurons une sauvegarde au niveau des partages de fichiers et sur les services de stockage eux-mêmes pour assurer la sauvegarde la plus complète afin de répondre à tous les scénarios de suppression volontaires ou involontaires de fichiers ou de services.

Suppression des fichiers

Les fichiers sont sauvegardés sur des partages de fichiers créés dans des comptes de stockage « Azure Files ».

Un mécanisme de suppression réversible (Soft Delete en anglais) est configuré sur les partages de fichiers Azure Files et permet de restaurer les fichiers supprimés pendant 365 jours.

La suppression réversible permet de récupérer les fichiers lorsqu'ils ont été supprimés par erreur par une application ou un utilisateur. Le mécanisme de suppression réversible ne supprime pas les données physiquement, elles sont mises dans un état de sommeil et invisible aux différents services. La suppression définitive est réalisée à la fin de la période de réversibilité.

Les spécifications techniques sont disponibles ici :

<https://learn.microsoft.com/fr-fr/azure/storage/files/storage-files-prevent-file-share-deletion>

Modification des fichiers

Nous mettons en œuvre une politique de sauvegarde au niveau du partage de fichier dans les comptes de stockage qui hébergent les fichiers de l'application.

Cette politique consiste en une sauvegarde quotidienne avec une rétention à 14 jours.

<https://learn.microsoft.com/fr-fr/azure/backup/azure-file-share-backup-overview>

Sécurisation des services de stockage

Au-delà des mécanismes de sauvegarde activé sur les partages de fichiers Azure Files, les services Azure Files exploités par Silae sont eux-mêmes sécurisés et sauvegardés avec Azure Recovery Service. L'intégralité des stockages et des services de stockage sont sauvegardés.

Ce mécanisme offre une double protection au niveau des fichiers et au niveau des services opérant ces fichiers. Azure Recovery Service expose un mécanisme de suppression réversible exploité par Silae. Si un intervenant malveillant supprime complètement un compte de stockage (ou même si le compte de stockage est accidentellement supprimé), les données du service sont intégralement conservées pendant 14 jours supplémentaires, ce qui permet la récupération de cet élément sans aucune perte de données.

Les spécifications techniques de Azure Recovery Service sont disponibles ici : <https://docs.microsoft.com/fr-fr/azure/backup/backup-azure-recovery-services-vault-overview>

Les sauvegardes de fichiers sont systématiquement chiffrées au repos avec des clés de chiffrement basées sur l'algorithme AES 256.

9.4. Restauration des Fichiers

Silae s'engage à restaurer les fichiers sur la base de la sauvegarde la plus appropriée avec un RTO (Recovery Time Objective) maximum de 24 heures, et ce, dans les meilleurs délais.

Restauration d'un fichier supprimé

- Le RPO minimal pour la restauration d'un fichier correspond à sa date de suppression dans la limite de 365 jours.

Restauration d'une version antérieure d'un fichier

- Le RPO minimal pour la restauration d'une version antérieure d'un fichier correspond à l'heure de la dernière sauvegarde dans la limite de 24 heures.
- La perte de données maximale est donc de 24 heures.

10. MISE A JOUR

Silae est responsable de la Mise à Jour du Service et effectue les Mises à Jour sans autorisation préalable du Client.

Il existe deux types de Mises à Jour :

- Les mises à jour hebdomadaires liées à l'amélioration continue de l'application.
- Les correctifs (patches applicatifs).

La version de l'application évolue à chaque Mise à Jour et est consultable dans l'application.

Les Mises à Jour hebdomadaires sont déployées pendant les Périodes de Maintenance Standard et peuvent entraîner une interruption de service.

Les correctifs sont déployés au plus tôt, selon l'urgence et la criticité. Dans la mesure du possible, les correctifs sont publiés lors de Périodes de Maintenance Standard. Les correctifs peuvent entraîner une Maintenance Planifiée ou Urgente à tout moment.

Les informations liées au contenu des Mises à Jour sont disponibles dans le Centre d'Aide accessible depuis l'application.