## 1. QUALIFICATIONS DES ADMINISTRATEURS DU CLIENT

Seuls les Collaborateurs à profil "Administrateur" ont accès à la Maintenance, mais en aucun cas les Collaborateurs à profil "Utilisateur".

Il appartient au Client de veiller à ce que ses Administrateurs disposent effectivement chacun et en permanence des compétences individuelles, niveau d'habilitation, certifications ou qualifications nécessaires ou requises pour accéder aux prestations de Maintenance. WALLIX se réserve le droit de bloquer l'accès aux prestations de Maintenance à toute personne qui ne justifierait pas de la qualité d'Administrateur du Client ou à des Administrateurs qui ne disposeraient pas de la qualification nécessaire à l'utilisation du Service.

Le Client transmet si nécessaire la liste limitative des Administrateurs qui sont seuls autorisés à accéder aux prestations de Maintenance. Cette liste doit être tenue à jour par le Client et envoyé en tant que de besoin à WALLIX.

## 2. SUPPORT

Le Support en ligne de WALLIX est le premier service accessible aux Collaborateurs à profil "Administrateur" du Client à partir du Portail Client https://support.wallix.com afin :

(i) d'accéder à l'ensemble de la Documentation du Service (installation, utilisation, etc.),

(ii) d'accéder à des espaces de lecture et de discussion en ligne : base de connaissance, formation en ligne, etc. au fur et à mesure que WALLIX et son écosystème y ajoutent des contenus gratuits, et

(iii) d'enregistrer et de suivre ses tickets de demande de Support et de Maintenance.

Si la question/demande n'est pas résolue par les ressources en ligne, le Client accède au service de Support comme ci-après décrit.

Pour tout problème relatif à l'installation ou à l'utilisation du Service, l'Administrateur peut soumettre à WALLIX un ticket de Support, via un des canaux disponibles, à savoir par téléphone ou à partir du Portail Client).

WALLIX s'engage à prendre en compte les tickets d'incident 24h/7j/365j et dans un délai de 2h à compter de leur ouverture.

La langue utilisée dans le cadre du Support est l'anglais.

## 3. DIAGNOSTIC

Seuls les profils Administrateur du Client ont accès au Service Support, mais en aucun cas les autres Collaborateurs du Client.

A réception du ticket d'incident, WALLIX opère un diagnostic sur le problème du Client, le qualifie puis oriente l'Administrateur du Client vers :

(i) un contenu accessible depuis le Support en ligne, ou

(ii) une prestation de Support, ou

(iii) une prestation de Maintenance, ou

(iv) une prestation complémentaire au sens de l'article Services Professionnels des CGU dans le cas où l'incident ne relèverait pas du Service.

Dans l'hypothèse où l'incident ne relèverait pas du Service, WALLIX se réserve la faculté de refacturer au Client les coûts générés par la prise en charge du ticket et le diagnostic de l'incident.

## 4. ENGAGEMENTS DU CLIENT

Pour bénéficier de la Maintenance dans le respect des Niveaux de service définis à l'ANNEXE « Niveau de Service (SLA), l'Administrateur du Client est tenu de signaler au plus vite à WALLIX tout incident à compter de sa découverte en ouvrant un ticket d'incident.

Une fois l'incident pris en compte par WALLIX, l'Administrateur s'engage, dans le cadre de son obligation de collaboration, à :

(i) transmettre sans délai à WALLIX toute information utile pour que WALLIX puisse reproduire ledit incident, notamment un descriptif précis de l'incident, les fichiers de logs, la configuration mise en place, et les circonstances de sa survenance (heure précise…) ;

(ii) se rendre disponible à l'égard de WALLIX, et permettre à WALLIX de se mettre en relation avec toute personne susceptible de lui fournir toute information utile sur l'incident signalé afin d'en assurer la reproduction.

Le Client reconnaît que sa collaboration est essentielle dans la résolution des incidents, tout retard ou imprécision de sa part, ainsi que tout défaut de signalement, exonérant WALLIX de sa responsabilité au titre des niveaux de services et/ou plus généralement de la Maintenance et du rétablissement du Service.

## 5. NIVEAU DE SEVERITE DU BUG OU DE GRAVITE DE LA VULNERABILITE

Une fois le ticket d'incident qualifié de Maintenance par le Service Support, WALLIX fixe le niveau de sévérité du Bug, ou de la Vulnérabilité connu(e) en l'État de l'Art selon les principes suivants :

### 5.1. Niveaux de sévérité du Bug

- S1 - Critique : Ce défaut indique une indisponibilité complète du produit ou du service.
- S2 - Sévère : C'est un défaut visible et impactant, qui arrête ou entrave significativement une fonctionnalité majeure. Cependant, d'autres parties du système restent fonctionnelles.
- S3 - Normal : Il provoque un comportement indésirable dans une fonctionnalité, mais le système reste fonctionnel.
- S4 - Faible : Inconvénient ou erreur, tandis que le système reste fonctionnel.

### 5.2. Gravité de la Vulnérabilité

**(i)** **Bloquante** : score CVSS égal ou supérieur à 9;
**(ii)** **Majeure :** score CVSS entre 8 (inclus) et 9 (exclu);
**(iii)** **Mineure** : score CVSS inférieur à 8.

## 6. ETAT DE L'ART

L'État de l'Art des techniques de développement et de correction des programmes d'ordinateur ne permet pas à WALLIX de pouvoir corriger de manière définitive la totalité des Bugs (en ce compris toute Vulnérabilité et tout Malware) susceptibles d'affecter le Service et/ou le Logiciel. En signant le Contrat, le Client reconnaît expressément accepter l'aléa inhérent à la qualité des prestations rendues par WALLIX au titre de la Licence d'Utilisation et de la Maintenance.

Une Vulnérabilité connue en l'État de l'Art est un Bug au sens du Contrat lorsqu'elle impacte le Service et/ou le Logiciel, que WALLIX s'engage à corriger dans le cadre de ses obligations de Maintenance. Entre les parties, une Vulnérabilité est une Information Confidentielle au sens du Contrat. D'un commun accord des parties, la criticité d'une Vulnérabilités est appréciée selon la méthode N.I.S.T CVSS (Common Vulnerability Scoring System) version 3.x.

Que ce soit au titre de la Licence d'Utilisation ou de la Maintenance, WALLIX n'est en aucune manière responsable des conséquences ni de la présence dans le Service et/ou le Logiciel d'un Malware ou d'une Vulnérabilité inconnu(e) en l'État de l'Art, ni de l'éventuelle Compromission du Système d'Information du Client en découlant.

## 7. MAINTENANCE

WALLIX procède à l'installation des mises à jour des versions, tant mineures que majeures, dès lors que celles-ci sont disponibles à son catalogue.

WALLIX s'engage à informer le Client d'une Maintenance programmée dans un délai d'un (1) mois avant la plage d'interruption prévue.

A titre exceptionnel, dans l'hypothèse où le Client serait dans l'impossibilité d'accepter la plage horaire d'interruption du Service pour des motifs légitimes, il pourra demander un report de l'interruption de maximum deux (2) mois, étant précisé que la plage d'interruption sera définie d'un commun accord entre WALLIX et le Client.

Le Client ne peut s'opposer à une mise à jour, sauf à perdre le bénéfice de la Maintenance.

## 8. CONDITIONS DE RESOLUTION D'UN INCIDENT

### 8.1. Bug ou Vulnérabilité du Logiciel

WALLIX s'engage à faire ses meilleurs efforts pour corriger les Bugs ou Vulnérabilités constatés, en fonction du niveau de sévérité du Bug ou du niveau de gravité de la Vulnérabilité.

Suite à l'examen de l'ensemble des éléments relatifs à l'incident, WALLIX pourra procéder aux modifications nécessaires sur le Logiciel, sur la configuration du Logiciel ou si nécessaire, adresser au Client toutes demandes de mise en œuvre de procédures destinées à apporter une solution à l'incident, y compris de contournement. Le Client s'engage à ce titre à exécuter les instructions et directives de WALLIX. Le cas échéant, WALLIX pourra programmer la correction de l'incident lors d'une prochaine mise à jour du Logiciel.

### 8.2. Incident sur l'infrastructure du Service

#### 8.1.1. Correctifs du Service

Les correctifs du Service sont installés et mis en production sur la Plateforme de l'Hébergeur par WALLIX, sans intervention du Client.

Le Client sera contacté au minimum 5 jours ouvrés avant le début d'une Maintenance du Service. Les détails du correctif et le processus de mise à jour du Service du Client, lui seront présentés.

L'application de correctif peut entrainer une interruption de Service. Dans ce cas précis, le Client sera tenu au courant lors de la présentation du processus d'application du correctif, avec une prévision du temps d'indisponibilité.

#### 8.1.2. Objectif de Temps de Reprise (OTR)

Afin de réduire l'impact de l'incident sur l'utilisation du Service par le Client, WALLIX se réserve le droit de recourir à une solution temporaire de contournement dans l'attente de la fourniture d'un correctif.

WALLIX s'engage à restaurer une continuité du service du Client dans un délai de 4 heures à compter du moment où :

- L'incident est identifié comme étant lié au Service et/ou à l'infrastructure opéré(e) par WALLIX.
- L'incident n'a pas été produit par une mauvaise utilisation du Service par le Client.

La valeur maximale de l'**OTR** est de 4 heures.

#### 8.1.3. Objectif de Point de Reprise (OPR)

Une sauvegarde du service du Client est réalisée par WALLIX tous les jours à 03h. Cet horaire suit la région où sera déployé le service du Client.

Les sauvegardes du service du Client sont stockées 30 jours par WALLIX. Les sauvegardes qui existent depuis plus de 30 jours sont automatiquement supprimées.

Si un incident se produit sur le service du Client avant l'heure de sauvegarde (i.e. 03h), WALLIX s'engage à restaurer le service avec la sauvegarde la plus récente disponible (J-1).

La valeur maximale de l'**OPR** est de 24 heures.

#### 8.1.4. Poursuite du Service en cas de manquement

Dans le cas où le Client aurait à remédier à manquement contractuel, notamment à un défaut de paiement, dans les conditions et délais tels que prévus au Contrat, le Service sera maintenu pendant toute la durée du manquement, jusqu'à sa remédiation par le Client ou jusqu'à la résiliation du Contrat, les Redevances restant dues par le Client conformément au Contrat.

#### 8.1.5. Conservation des Données à la fin du Contrat

WALLIX s'engage à supprimer toutes Données du Client dans un délai de maximum de 90 jours à compter de la résiliation ou de l'expiration du Contrat. Au-delà de ce délai, le Client ne pourra solliciter la restitution de ses Données qui seront supprimées.

Toute demande de restitution de Données doit être formalisée par écrit et notifiée à WALLIX dans un délai maximum de 30 jours à compter de la date de résiliation ou d'expiration du Contrat. Au-delà de ce délai, WALLIX se réserve le droit de ne pas accéder à la demande du Client et/ou n'assure pas la disponibilité des Données du Client.

Sans que cette liste ne soit exhaustive, les Données du Client qui seront supprimées à l'échéance du Contrat sont les suivantes :

- Sauvegardes
- Données d'utilisation du Service/de la Licence d'utilisation
- Documentation d'architecture
- Documentation de flux
- Documentation opérationnelle
- Nom, contact & informations du Client / point de contact
- IP et informations réseaux du Client

## 9. EXCLUSIONS

En toute hypothèse, WALLIX ne peut être tenue responsable ni prendre en charge, au titre de la restauration du Service ou de la Maintenance tout incident liée à (i) une utilisation du Logiciel non conforme à sa destination, à sa Documentation ou aux préconisations de WALLIX, (ii) une panne matérielle ou logicielle d'un ou plusieurs éléments du système informatique ou réseau du Client, (iii) une défaillance des réseaux de communications électroniques, ralentissement ou engorgement du réseau internet ou du réseau du Client, (iv) un paramétrage de l'environnement informatique ou des postes du Client, (v) un refus du Client de collaborer avec WALLIX dans la résolution des incidents, (vi) une incompatibilité entre le Service et de nouveaux matériels ou logiciels tiers mis en œuvre par le Client sans validation préalable par WALLIX, (vii) une contamination du système informatique du Client par un virus informatique, (viii) un acte de piratage ou une intrusion frauduleuse dans le système informatique du Client, (ix) l'intervention d'un tiers sur le Service non autorisée par WALLIX, (x) et plus généralement à tout acte volontaire de dégradation, malveillance, sabotage du Client ou d'un tiers, ou détérioration due à un cas de force majeure.

En cas de dysfonctionnement dû à l'un de ces cas, le Client peut demander à WALLIX une tentative de remise en état sur la base d'une proposition commerciale de Services Professionnels.

En cas de modification de son système informatique par le Client, celui-ci en informe au préalable WALLIX par écrit, dès lors que cette modification est susceptible d'avoir un impact sur le fonctionnement du Service ou

l'exécution de sa Maintenance. Le cas échéant, WALLIX notifie alors au Client, sous quinze (15) Jours ouvrés à compter de la réception de l'information du Client, les conséquences techniques ou tarifaires de la Maintenance qui seraient induites par la modification du système du Client. A défaut d'information par le Client, WALLIX dégage toute responsabilité dans l'utilisation du Service et dans l'exécution de sa Maintenance, ce que le Client reconnaît.

## 10. EVOLUTION DU SERVICE

L'évolution du Service est effectuée selon la feuille de route (roadmap) définie par WALLIX, et est prise en compte dans la Redevance. WALLIX procède seul à l'installation des mises à jour et/ou nouvelles versions directement sur l'infrastructure, à fonctionnalités et performances équivalentes. Le Client bénéficie ainsi des améliorations du Service sans avoir à installer de nouvelle version de la Solution, WALLIX prenant en charge cette évolution par télémaintenance.

L'évolution du Service ne comprend pas les éventuelles demandes fonctionnelles spécifiques du Logiciel que le Client souhaiterait, ni la mise à niveau des Logiciels Tiers en cas d'évolution du Service, ni la mise à niveau du Service en cas d'évolution des Logiciels Tiers. Le cas échéant, le Client expose son besoin à WALLIX qui émet une proposition commerciale de Services Professionnels distincte pour les développements spécifiques ou adaptations à effectuer sur le Logiciel. Si le Client confirme par écrit qu'il passe commande de Services Professionnels, WALLIX installe le développement spécifique ou l'adaptation sur l'infrastructure, et le Client y accède via sa connexion au Service, sous réserve de s'acquitter du prix desdits Services Professionnels spécifiques. Tout développement ou adaptation spécifique fait l'objet d'une recette par le Client.

## 1. Taux de disponibilité

A compter de la Date de Mise en Production du Service, WALLIX s'engage à assurer un pourcentage de temps de disponibilité mensuel minimum de 99,9%.

Conformément à l'article 5 des CGU, le temps de disponibilité ne tient pas compte des opérations de Maintenance du Service ou des interruptions de fonctionnement de l'Internet.

Le taux de disponibilité du Service (SLA) est calculé "départ Plateforme" (sortie datacenter), sur la base d'un (1) mois civil de trente (30) jours, en soustrayant le temps d'indisponibilité du Service en minutes de la disponibilité totale en minutes équivalent à 24h/24 et 7j/7.

## 2. Non-respect du taux de disponibilité, pénalités et Avoir de temps de Service

En cas de non-respect par WALLIX du taux mensuel de disponibilité du Service, le Client peut faire, dans un délai de trente (30) jours suivant la fin du mois calendaire concerné, une demande d'Avoir de temps Service équivalent à une prorogation de la durée du Service par WALLIX du Service, en plus de la Durée Initiale ou de la Période Additionnelle concernée et sans Redevance supplémentaire, et ce, quel que soit le nombre de Collaborateurs affectés selon la formule suivante :

(i) Taux d'indisponibilité mensuel entre 99,9 et 99% : 1 jour de Service ;
(ii) Taux d'indisponibilité mensuel entre 99% et 95% : 3 jours de Service ;
(iii) Taux d'indisponibilité mensuel inférieur à 95% : nombre de jours d'indisponibilité x 3 et plafonné à quinze (15) jours de Redevance.

La demande d'Avoir de temps de Service doit être adressée au Service Support de WALLIX et inclure toutes les informations nécessaires pour permettre de valider la réclamation, y compris une description détaillée de l'incident, des informations sur l'heure et la durée de l'indisponibilité du Service.

Dans les trente (30) jours de réception de la demande du Client, WALLIX s'engage à y répondre de bonne foi et, en cas de réponse positive, validera l'Avoir de temps de Service et rendra le Service pendant la durée additionnelle correspondante. Tout Avoir de temps de service non réclamé sera perdu à la date d'échéance de la Durée Initiale (ou de toute Période Additionnelle).

## 1. PERIODE D'ESSAI – TEST

Si le Client utilise une version d'essai, WALLIX met cette version d'essai à la disposition du Client pour une période se terminant à la première des dates suivantes :

- la fin de la période d'essai gratuit ou de la période de preuve de concept (POC), telle que communiquée par WALLIX ou spécifiée dans une Commande ;
- la date de début de toute version achetée du Logiciel ; ou
- la notification écrite de résiliation par WALLIX.

Pendant la période d'essai, WALLIX accorde au Client une licence non exclusive et non transférable, sans droit de sous-licence, pour accéder à la version d'essai et l'utiliser à des fins d'évaluation des besoins internes du Client conformément à la Documentation et sous réserve des restrictions d'utilisation énoncées dans le présent Contrat. Le Client doit utiliser la version d'essai uniquement à des fins d'évaluation et non à des fins commerciales ou productives, sauf autorisation écrite contraire de WALLIX.

WALLIX fournit la version d'essai " en l'état " sans aucune garantie ou représentation de quelque nature que ce soit. Dans les limites autorisées par la loi, WALLIX rejette toutes les garanties et représentations implicites, y compris, mais sans s'y limiter, les garanties implicites de commercialisation, d'adéquation à un usage particulier et de sécurité.

Le défaut de réserves écrites et documentées pendant la période d'essai, vaut recette sans réserve du Service par le Client. Passée la fin de la période d'essai, toute réserve relative au fonctionnement du Service sera traitée par WALLIX dans le cadre des prestations mentionnées dans l'ANNEXE « Maintenance ».

Le paramétrage préalable du Service avant la Mise en Production peut être un élément déterminant de son bon fonctionnement. Ce paramétrage est assuré par le Client, sous sa responsabilité, éventuellement avec l'assistance de WALLIX dans le cadre de Service Professionnel. Toute modification ultérieure des paramètres du Service sera de la seule responsabilité du Client.

## 2. DETAIL DES DROITS CONCEDES

Pendant la durée du Contrat, WALLIX concède au Client une Licence d'Utilisation sur le Logiciel utilisé pour rendre le Service qui comprend le droit d'utiliser le Logiciel seulement en version binaire, de manière non exclusive et non transférable, qui ne peut faire l'objet d'une sous-licence, d'une cession, d'un transfert ou d'une mise à disposition d'un tiers, à titre gratuit ou onéreux, selon quelque modalité pratique ou juridique que ce soit (sauf disposition expresse en sens inverse dans le Contrat).

Le coût de la Licence d'Utilisation du Logiciel utilisé pour rendre le Service est inclus dans le montant de la Redevance.

Le Service est destiné à être utilisé par le Client seulement pour le traitement de ses Données dans les conditions limitativement définies au Contrat.

De convention expresse entre les parties, la Licence d'Utilisation sur le Logiciel utilisé pour rendre le Service constitue une mise à disposition d'un exemplaire du Logiciel et non une cession des droits de propriété intellectuelle.

WALLIX se réserve le droit (i) de faire évoluer les fonctionnalités du Logiciel sans retrait des principales fonctionnalités décrites dans les CGU, ni abaissement du niveau de Sécurité et (ii) de proposer au Client de nouvelles fonctionnalités, éventuellement soumise à paiement d'une Redevance supplémentaire.

## 3. LPM - SIIV ET ACCES AUX CODES SOURCE

Conformément à l'article R.1332-41-13 Code de la défense (LPM 2013) pour le cas où le Logiciel serait installé dans le périmètre du Système d'Information d'Importance Vitale du Client, WALLIX s'engage à tenir à disposition de l'ANSSI la version des codes source du Logiciel utilisé par le Client dans le cadre du Service.

## 4. GARANTIE DE JOUISSANCE PAISIBLE

WALLIX garantit (i) que le Logiciel utilisé pour rendre le Service est original et (ii) être titulaire de l'intégralité des droits de propriété intellectuelle sur le Logiciel, sous réserve des éventuels modules intégrés au Logiciel qui bénéficieraient d'une licence de type "Open Source" (à effet non contaminant) et identifiés à l'article Conditions Particulières ou (iii) disposer du droit de concéder une Licence d'Utilisation au Client sur les éventuels modules du Logiciel dont les droits de propriété intellectuelle sont détenus par un tiers, de manière à ce que WALLIX puisse valablement, à son tour, en concéder l'utilisation au Client dans les conditions de la Licence d'Utilisation détaillée dans l'ANNEXE MAINTENANCE.

WALLIX s'engage à n'utiliser aucun logiciel en licence Open Source à effet contaminant.

Pendant la durée du Contrat, WALLIX garantit le Client contre toute action ou procédure judiciaire au motif d'une éventuelle atteinte par le Logiciel aux droits de propriété intellectuelle d'un tiers. WALLIX se charge, à ses frais et à son choix, de la défense à conduire du fait de l'action menée à l'encontre du Client par ce tiers.

En cas de condamnation civile de WALLIX par décision de justice ayant autorité de la chose jugée au principal et passée en force de chose jugée ou en cas de transaction conclue par WALLIX, WALLIX pourra, à son choix et à ses frais, soit (i) obtenir pour le Client le droit de continuer à utiliser le Logiciel (i) sans augmentation du montant de la Redevance et (ii) et sans interruption d'usage du Service pour le Client, éventuellement en modifiant tout ou partie du Logiciel pour qu'il ne constitue plus une contrefaçon des droits du tiers.

Si le droit de continuer à utiliser le Logiciel ne peut être obtenu ou si le Logiciel ne peut être remplacé ou modifié pour un coût raisonnable pour WALLIX afin de ne plus constituer la contrefaçon des droits du tiers, WALLIX pourra notifier au Client la résiliation du Contrat et restituer au Client le montant total de la Redevance payée d'avance par le Client, prorata temporis à compter de la date de la réclamation du tiers (période postérieure à la dernière prestation n'ayant pas reçu sa contrepartie), nonobstant le droit pour le Client de solliciter l'indemnisation judiciaire de son entier préjudice.

## 5. LIMITES STRICTES

Le strict respect par le Client de la propriété intellectuelle de WALLIX et les conditions dans lesquelles WALLIX accorde au Client une Licence d'Utilisation sur le Logiciel constituent ensemble une qualité essentielle expresse de la prestation du Client attendue par WALLIX.

Toute modification ou toute tentative de modification par le Client des conditions d'utilisation du Service (durée d'utilisation, accès par un moyen non autorisé ou non prévu par WALLIX, augmentation non autorisée par le Client du nombre de Collaborateurs habilités à utiliser le Service , etc.) ou toute utilisation du Service dans des conditions non prévues au Contrat, sans l'accord préalable et écrit de WALLIX, représente un danger considérable pour la pérennité de l'entreprise de WALLIX dont la propriété intellectuelle sur le Logiciel constitue un actif essentiel et est réputée constituer une inexécution suffisamment grave de la part du Client pour entraîner le droit pour WALLIX de suspendre immédiatement et de plein droit la prestation du Service et la Licence d'Utilisation du Logiciel dès la date d'envoi d'une information en ce sens par WALLIX au Client, notamment par courrier électronique, confirmée par notification.

| Domaine | Mesures opérationnelles |
|---|---|
| Organisation de la sécurité de l'information | **Responsabilité de la Sécurité** : WALLIX a désigné un responsable de la sécurité (CISO) pour superviser, mettre en œuvre et gérer les règles, politiques et procédures de sécurité. Le cadre documentaire de sécurité est aligné par rapport à la norme ISO27001.<br><br>**Programme de Gestion des Risques :** Avant de traiter les données clients ou de lancer les services en ligne, WALLIX réalise une évaluation des risques. Les scénarios de risques identifiés couvrent les dommages sur site, les cyberattaques et les risques liés au personnel.<br><br>**Comitologie de Sécurité** : des comités de sécurité dédiés sont mis en place pour gérer la sécurité dans le cadre de l'application SAAS de WALLIX. Un comité Direction établit la gestion des risques, les objectifs de sécurité et les politiques ; une instance opérationnelle est utilisée pour mettre en œuvre la sécurité et les contrôles de sécurité au fil du temps.<br><br>**Cycle de vie des documents** : WALLIX tient à jour ses documents de Sécurité annuellement. |
| Gestion des actifs | **Inventaire des actifs :** WALLIX tient un registre de tous les actifs contenant des données Clients ou utilisés pour administrer des systèmes en production. Chaque actif est attaché à un responsable en charge du maintien de l'actif au bon niveau, notamment de sécurité.<br><br>**Gestion des actifs**<br><br>- WALLIX classe les Données Clients comme confidentielles et maintient un accès strictement restreint aux équipes autorisées.<br>- WALLIX interdit strictement l'exportation de données de production en dehors des environnements de production.<br>- Par défaut, tous les systèmes mettent en œuvre : des scans de vulnérabilité, une gestion des correctifs, une gestion de la configuration, une gestion des accès, une gestion des journaux et un durcissement du système. |
| Sécurité des Ressources Humaines | **Rôles et responsabilités** : Les membres du personnel de WALLIX ayant accès aux données clients sont liés par des obligations de confidentialité dans le cadre de leur contrat.<br><br>**Formation en sécurité** : WALLIX forme son personnel aux procédures de sécurité adaptées et à leurs rôles respectifs en matière de sécurité. WALLIX informe également son personnel des conséquences possibles en cas de violation des règles et procédures de sécurité. WALLIX n'utilisera que des données anonymes dans le cadre de la formation. Le CISO établit un plan de sensibilisation annuel et obtient l'approbation de l'EXCOM.<br><br>**Formation en sécurité dédiée** : Le programme de sensibilisation couvre les meilleures pratiques en matière de sécurité et la formation spécifique liée aux descriptions de poste des collaborateurs. Pour les applications SAAS, les procédures et politiques spécifiques mises en œuvre sont couvertes par le plan de sensibilisation. |
| Sécurité physique et environnementale | **Accès physique aux installations**. WALLIX tient à jour la référence des centres de données et des fournisseurs de services cloud utilisés pour traiter les données clients. Toutes les installations se trouvent en Europe et démontrent un niveau de sécurité adéquat avec au moins les certifications ISO27001.<br><br>**Protection contre les interruptions.** WALLIX n'utilise que des fournisseurs de services cloud qui démontrent une assurance concernant les risques de perte de données par le biais d'un programme de certification approprié.<br><br>**Bureaux de WALLIX :** L'environnement traitant les données clients est administré depuis une salle dédiée accessible uniquement au personnel autorisé. Les contrôles suivants sont mis en place : contrôle d'accès nominatif + enregistrement vidéo + détection d'intrusion. Les fichiers journaux sont conservés pendant 6 mois. |
| Gestion de la communication et des opérations | **Politique opérationnelle**. : WALLIX tient à jour des documents de sécurité décrivant ses mesures de sécurité et les procédures et responsabilités adaptées applicables au personnel ayant accès aux données clients.<br><br>**Procédure de Récupération des Données**<br><br>- de manière régulière, et en aucun cas moins d'une fois par jour, WALLIX tient à jour plusieurs copies des Données Clients à partir desquelles de telles Données peuvent être récupérées.<br>- WALLIX conserve des copies des Données Clients et des procédures de récupération des Données sur un site de sauvegarde à partir duquel l'équipement principal traitant les Données Clients est situé.<br>- WALLIX restreint l'accès aux copies des Données Clients au personnel ayant accès à la production.<br><br>**Logiciels malveillants** : WALLIX utilise des systèmes segmentés et renforcés pour traiter les Données. L'accès à la base est limité aux équipes d'infrastructure via un Bastion interne WALLIX. Cet accès est uniquement autorisé que pour installer des logiciels administratifs provenant de référentiels officiels et de vérifier les signatures binaires via une procédure de gestion des modifications. |

| Domaine | Mesures opérationnelles |
|---|---|
| | Les accès distants aux applications sont contrôlés via des pares-feux, des serveurs proxy inversés et des pare-feu d'applications web.<br><br>**Données transfrontalières**<br><br>WALLIX chiffre toutes les données transmises sur les réseaux publics. Seuls les protocoles chiffrés sont utilisés.<br><br>WALLIX contrôle l'accès à l'environnement de production limitant l'exposition via un Bastion. Il est configuré pour exporter ses journaux et fournir un enregistrement des sessions.<br><br>**Journalisation des événements**<br><br>WALLIX journalise, ou permet au client d'enregistrer dans des fichiers journaux, l'accès et l'utilisation des Systèmes d'Information contenant les Données Clients, les fichiers journaux étant disponibles pour le Client pendant 3 mois et pouvant être récupérés pendant un an. |
| Contrôle d'accès | **Politique d'accès**<br><br>WALLIX tient à jour un registre des privilèges de sécurité des individus ayant accès aux Données Clients.<br><br>**Autorisation d'accès**<br><br>- WALLIX tient à jour un registre du personnel autorisé à accéder aux systèmes WALLIX contenant des Données Clients.<br>- WALLIX désactive les identifiants d'authentification qui n'ont pas été utilisés pendant une période n'excédant pas six mois.<br>- WALLIX identifie le personnel qui peut accorder, modifier ou annuler l'accès autorisé aux données et aux ressources.<br>- L'équipe chargée de contrôler l'accès à l'environnement de production est dédiée et isolée de l'équipe de production SAAS.<br><br>**Principe du moindre privilège**<br><br>- Le personnel de Support technique n'est autorisé à accéder aux Données Clients que lorsque cela est nécessaire.<br>- WALLIX limite l'accès aux Données Clients uniquement aux personnes qui en ont besoin pour accomplir leur mission.<br>- L'équipe chargée de mettre en place l'accès à l'environnement de production est isolée de l'équipe de production SAAS. Les utilisateurs qui mettent en place l'accès ne sont pas les utilisateurs qui utilisent l'accès.<br><br>**Intégrité et confidentialité**<br><br>- WALLIX applique une configuration pour désactiver les sessions d'administration lorsqu'un individu quitte les locaux contrôlés par WALLIX ou lorsqu'un ordinateur est laissé sans surveillance.<br>- WALLIX stocke les mots de passe de manière à ce qu'ils soient inintelligibles tant qu'ils sont en vigueur.<br><br>**Authentification**<br><br>- WALLIX utilise des pratiques conformes aux normes de l'industrie pour identifier et authentifier les utilisateurs qui tentent d'accéder aux Systèmes d'Information.<br>- Lorsque les mécanismes d'authentification reposent sur des mots de passe, WALLIX exige que le mot de passe ait au moins 14 caractères. L'authentification multifactorielle est obligatoire.<br>- WALLIX veille à ce que les identifiants désactivés ou expirés ne soient pas attribués à d'autres individus.<br>- WALLIX tient à jou des procédures conformes aux normes de l'industrie pour désactiver les mots de passe qui pourraient avoir été corrompus ou divulgués accidentellement.<br>- WALLIX utilise des pratiques de protection des mots de passe conformes aux normes de l'industrie, y compris des pratiques conçues pour maintenir la confidentialité et l'intégrité des mots de passe lors de leur attribution et de leur distribution, ainsi que lors de leur stockage.<br><br>**Conception du réseau**<br><br>- WALLIX dispose de contrôles pour éviter que des individus n'utilisent des droits d'accès qui ne leur ont pas été attribués pour accéder à des Données Clients auxquelles ils ne sont pas autorisés. Les réseaux productifs sont |

| Domaine | Mesures opérationnelles |
|---|---|
| | strictement séparés des autres réseaux, nécessitant une autorisation pour mettre en œuvre les flux entrants et sortants.<br>- WALLIX restreint l'accès à l'infrastructure de production à l'infrastructure d'administration accessible uniquement à l'aide d'une Bastion.<br>**Accès à distance** : Tout accès à distance à l'infrastructure d'administration est contrôlé via un VPN dédié appliquant les meilleures pratiques en matière de sécurité. |
| Prévention et gestion des Incidents de Sécurité | **Gestion du changement:**<br>- Toutes les modifications sont traitées via une procédure de gestion du changement. Les modifications non standard sont approuvées par un comité consultatif. Le CISO est un membre permanent de ce comité.<br>- Tous les composants sont testés, examinés et vérifiés par une équipe de sécurité avant d'être mis en œuvre en production.<br>**Procédure de réponse aux Incidents :**<br>- WALLIX tient à jour un registre des violations de Sécurité avec une description de la violation, la période, les conséquences de la violation, le nom du rapporteur et à qui la violation a été signalée.<br>- Pour chaque violation de Sécurité constituant un Incident de Sécurité, WALLIX notifiera selon le contrat et les canaux de support.<br>**Surveillance du service :**<br>La surveillance est mise en œuvre pour surveiller la bonne exécution des Services et la Sécurité. |
| Gestion de la continuité d'activité | - WALLIX établit des plans d'urgence et de contingence pour les installations dans lesquelles se trouvent les Systèmes d'Information de WALLIX qui traitent les Données Clients.<br>- Le stockage redondant de WALLIX et ses procédures de récupération des Données ont pour objectif de reconstituer les Données Clients dans leur état d'origine ou leur dernier état répliqué avant leur perte ou leur destruction.<br>- Lorsque cela est approprié, WALLIX teste son plan de reprise d'activité après sinistre au moins tous les 6 mois. |

# ANNEXE – PROTECTION DES DONNEES A CARATERE PERSONNEL

**Préambule : définitions spécifiques**

Aux fins de la présente Annexe le terme « Règlementation Données » désigne la règlementation applicable au Client en matière d'utilisation de Données Personnelles, et en particulier la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« LIL ») ainsi que toute réglementation destinée à la compléter ou à la remplacer, en particulier, le Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces Données (ci-après « RGPD »).

Par ailleurs, les termes « Données Personnelles », « Traitement », « limitation du Traitement », « Fichier », « Responsable du Traitement », « Sous-Traitant », « Destinataire », « Tiers », « Consentement », « Violation de Données à Caractère Personnel », « Autorité de contrôle », « Personnes concernées » ont la signification que leur donne le Règlement Général pour la Protection des Données.

Le termes « Contrat » et « Prestation » ont la signification que leur donne nos Conditions Générales (CLUF, CGS ou CGU).

## 1. Objet

Les présentes clauses constituent une Annexe au Contrat et ont pour objet de définir les conditions dans lesquelles, dans le cadre du Contrat qui les lie, WALLIX s'engage à effectuer pour le compte du Client les opérations de traitement de Données à caractère personnel définies ci-après, où le Client intervient en tant que Responsable de traitement et WALLIX en tant que sous-traitant.

Il ne traite pas des Données privées de salariés échangées dans le cadre des relations commerciales et contractuelles entre WALLIX et son Client dont les règles de protection sont définies dans le Contrat.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de Données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des Données - RGPD »).

## 2. Description du traitement faisant l'objet de la sous-traitance

Les Produits et Services fournis par WALLIX pour le compte du Client sont explicités dans le Contrat signé par les parties.

## 3. Données traitées

Les Données traitées par le Sous-traitant sont les noms, prénoms, adresses électroniques, numéros de téléphone, adresses IP, journaux et enregistrements de sessions des Utilisateurs ou Administrateurs du Produit et/ou Service.

## 4. Catégories de personnes concernées

Les Personnes Concernées sont les Utilisateurs et Administrateurs du Produit et/ou du Service.

## 5. Durée du Contrat

La présente Annexe entre en vigueur à compter de la signature du Contrat et pour la durée telle que définie au Contrat.

## 6. Obligations de WALLIX vis-à-vis du Client

### 6.1 Traitement des Données

WALLIX s'engage à :

- Traiter les Données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance
- Traiter les Données conformément aux instructions documentées du Client figurant au Contrat et définie entre les parties comme la réalisation de l'objet du Contrat d'une part et l'utilisation des Produits et Services conformément à leur Documentation d'autre part.

En cas d'instruction complémentaire souhaité par le Responsable de Traitement excédant les obligations contractuelles de WALLIX et non imposées par le RGPD, WALLIX adressera un devis correspondant à la mise en œuvre de ladite instruction.

Si WALLIX considère qu'une instruction complémentaire constitue une violation du règlement européen sur la protection des Données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des Données, il en informe immédiatement le Client.

En outre, si WALLIX est tenu de procéder à un transfert de Données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

### 6.2 Confidentialité des Données

WALLIX s'engage à :

- Garantir la confidentialité des Données à caractère personnel traitées conformément aux stipulations du Contrat et du présent article ; étant précisé que cette garantie s'applique toutes les Données à caractère personnel, notamment :
    - Les Données à caractère personnel transmises par le Responsable de Traitement ;
    - Les Données à caractère personnel accessibles dans le cadre de la mission effectuée pour le compte du Responsable de Traitement ;
    - Les Données à caractère personnel reçues d'un tiers, par exemple tout partenaire intégrateur, infogérant ou autre, dans le cadre de la mission effectuée pour le compte du Responsable de Traitement.
- Veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du Contrat et de la présente Annexe :
    - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
    - Reçoivent la formation nécessaire en matière de protection des Données à caractère personnel.
- Prendre en compte, s'agissant de ses outils, produits, applications, services et process, les principes de protection des Données dès la conception et de protection des Données par défaut ;
- Mettre en œuvre et maintenir en place des mesures techniques et organisationnelles appropriées de manière à ce que le traitement garantisse la protection des droits des personnes concernées et soit conforme aux textes susvisés en prenant, notamment, toutes les mesures de sécurité requises en vertu de l'article 32 du RGPD, et ce tout au long de l'exécution du Contrat, notamment afin de protéger les Données à caractère personnel contre toute perte fortuite, altération, divulgation à des tiers non autorisés.
- Faire respecter par son personnel, ses sous-traitants et de manière générale à tout tiers intervenant à sa demande, l'ensemble des obligations relatives à la protection des Données, telles que mentionnées dans le Contrat et la présente Annexe.

Toute évolution réglementaire en matière de protection des Données personnelles qui pourrait donner lieu à un renforcement des obligations de WALLIX au titre du présent article sera prise en compte et mise en œuvre par WALLIX à ses frais.

### 6.3 Sous-traitance

WALLIX peut faire appel à un autre sous-traitant (ci-après, « sous-traitant ultérieur ») pour la réalisation de certaines prestations et dans ce cas les prestataires sous-traitants ultérieurs sont mentionnés dans les Conditions Particulières. Le Client sera informé préalablement et par écrit de tout éventuel ajout ou remplacement de sous-traitants ultérieurs. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant, et le cas échéant les transferts de Données en dehors de l'Union Européenne.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent Contrat pour le compte et selon les instructions du Client. Il appartient à WALLIX de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du règlement européen sur la protection des Données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, WALLIX demeure pleinement responsable devant le Client de l'exécution par l'autre sous-traitant de ses obligations.

### 6.4 Droit d'information des personnes concernées

Il appartient au Client de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des Données.

### 6.5 Exercice des droits des personnes

Dans la mesure du possible, WALLIX doit aider le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit de accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des Données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès de WALLIX des demandes d'exercice de leurs droits, WALLIX doit adresser ces demandes dès réception par courrier électronique au Client.

### 6.6 Notification des violations de Données à caractère personnel.

WALLIX notifie au le Client toute violation de Données à caractère personnel dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance et par le moyen le plus rapide et le plus sûr. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification contient au moins :

- La description de la nature de la violation de Données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif de enregistrements de Données à caractère personnel concernés ;
- Le nom et les coordonnées du délégué à la protection des Données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de Données à caractère personnel ;
- La description des mesures prises ou que WALLIX propose de prendre pour remédier à la violation de Données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

### 6.7 Coopération de WALLIX dans le cadre du respect par le Client de ses obligations règlementaires.

Dans la mesure de son implication dans le traitement, WALLIX aide le Client pour la réalisation de analyses d'impact relative à la protection des Données.

Dans la mesure de son implication dans le traitement, WALLIX aide le Client pour la réalisation de la consultation préalable de l'autorité de contrôle.

### 6.8 Mesures de sécurité.

WALLIX s'engage à mettre en œuvre les mesures de sécurité décrites dans l'Annexe Plan d'Assurance Sécurité et dans la PSSI.

Des précautions complémentaires pourront être apportées si elles apparaissent nécessaires au vu des conclusions de l'analyse d'impact d'un nouveau traitement ou d'une modification apportée à un traitement existant.

### 6.9 Sort des Données

Au terme de la prestation de services relatifs au traitement de ces Données, WALLIX s'engage à renvoyer toutes les Données à caractère personnel au Client.

Dans la mesure où elles leur conservation ne serait pas nécessaire à WALLIX pour s'acquitter de ses obligations légales ou se protéger dans ses droits, le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information de WALLIX. Une fois détruites, WALLIX devra justifier par écrit de la destruction.

En cas de sous-traitance ultérieure, WALLIX fait son affaire de répercuter vers ceux-ci la présente obligation.

### 6.10 Délégué à la protection des Données

Conformément à l'article 37 du règlement européen sur la protection des Données, WALLIX a nommé un délégué à la protection des Données en la personne de Maitre Olivier Weber – privacy@wallix.com.

### 6.11 Registre des catégories de activités de traitement

WALLIX déclare tenir par écrit un registre de toutes les catégories de activités de traitement effectuées pour le compte du Client comprenant :

- Le nom et les coordonnées du Client pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des Données ;
- Les catégories de traitements effectués pour le compte du Client ;
- Le cas échéant, les transferts de Données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des Données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :

    - La pseudonymisation et le chiffrement des Données à caractère personnel ;
    - Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
    - Des moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
    - Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

### 6.12 Documentation

WALLIX met à la disposition du Client la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation de audits, y compris des inspections, par le Client ou un auditeur tiers agréé qu'il aura mandaté, et contribuer à ces audits.

## 7. Obligations du Client vis-à-vis de WALLIX

Le Client s'engage à :

- Fournir à WALLIX les Données visées au II des présentes clauses
- Documenter par écrit toute instruction concernant le traitement des Données par WALLIX
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des Données de la part de WALLIX.
- Superviser le traitement, y compris réaliser les audits et les inspections auprès de WALLIX.

## 8. Autorité de contrôle

Les parties ont choisi la CNIL comme autorité de contrôle de leur conformité RGPD.