Vous faciliter l'IT

Plan d'Assurance Sécurité (PAS)

Sécurité du Système d'Information

Table des matières

Ce Plan d'Assurance Sécurité est établi entre la SOCIETE et le CLIENT

1. Définitions

Cf. annexe Définitions applicable des Conditions Générales de Vente.

2. Objet du document

Ce document décrit les dispositions que la Société s'engage à mettre en œuvre pour répondre aux exigences de sécurité des Systèmes d'Information et des données gérées dans le cadre de ses prestations. Il définit en particulier l'organisation qui est mise en place, la méthodologie suivie pour gérer la sécurité et les mesures techniques, organisationnelles et procédurales misent en œuvre.

3. Documents de référence

Le référentiel documentaire du Système Sécurité Projet est constitué notamment par :

- Les devis et ou la proposition commerciale et ou le Contrat
- Conditions de Vente (CdV)
    - Conditions Générales de Vente, ses Conditions Particulières de Vente, ses Conditions Spécifiques de Vente et ses Annexes
- Le Plan d'Assurance Sécurité (PAS)
- Les Procès-Verbaux de Recette – VABF et VSR
- Le Cahier d'Exploitation (DOE ou DTI)
- Les comptes rendus de réunion nommés RIDA (Relevé d'Information / Décisions / Actions)
- Le Plan d'Actions Général pour le suivi des actions du projet

La liste des documents applicables et de référence n'est pas exhaustive et peut évoluer selon les contextes Client.

4. Conditions d'interventions

Toutes prestations réalisées dans le cadre du PAS, et non proposées dans le devis initial du projet concerné, fait l'objet d'une facturation supplémentaire au temps passé, par demi (½) journée minimum au tarif de chef de projet. Ces prestations concernent la rédaction de la documentation nécessaire au PAS, la préparation des réunions, la participation et l'animation des réunions, le compte-rendu des réunions, le suivi des actions liées au PAS, sans que cela soit exhaustif et limitatif.

5. Rappel des exigences

5.1. Exigences de sécurité nominale

✓ **Exigences de sécurité liées à la protection des données personnelles (RGPD)**

Le Règlement Général européen sur la Protection des Données (UE) 2016/679 du 24 mai 2016 est appliqué depuis le 25 mai 2018. Il consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des Données à Caractère Personnel (DCP), dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'UE. Il impose des obligations spécifiques aux sous-traitants qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements.

La CNIL édite un « Guide du sous-traitant » qui exprime, notamment, les exigences spécifiques liées aux traitements des données personnelles.

Les exigences de sécurité nominale ainsi que les conditions générales de ventes (CGV) tiennent compte des législations en vigueur et notamment du RGPD (UE) 2016/679.

Des compléments aux exigences de sécurité nominale peuvent exister dans les annexes métiers.

5.2. Exigences de sécurité spécifiques

Si le Client souhaite exprimer des exigences de sécurité particulières, il pourra le faire par le biais de l'***Annexe Mesures Spécifiques*** en accord avec la Société.

6. Organisation

Chacune des Parties nomme au sein de son organisation des interlocuteurs en charge du projet, le maintien à jour de cette liste est de la responsabilité des Parties, le changement d'interlocuteur ou le départ d'un interlocuteur doit être communiqué dans les meilleurs délais à l'autre Partie.

6.1. Organisation de la maîtrise d'œuvre :

En tant que maître d'œuvre, la Société désignera un interlocuteur « Responsable Sécurité Maitrise d'Œuvre » (RSMOE), pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité.

Le RSMOE prend en charge l'organisation des comités de suivi sécurité projet : convocation, proposition d'ordre du jour, rédaction des compte-rendu.

✓ **Instances de suivi de la sécurité du projet**

- Le suivi de la sécurité du projet est assuré par le RSMOE qui intègre des points sécurités lors des comités de pilotage/groupe opérationnel et comité de suivi.
- Un comité de sécurité peut être organisé à la demande la Société ou du Client pour revoir le PAS et l'amender.

Comité de sécurité	
Objet	C'est l'instance sécuritaire du projet. Il assure la maîtrise sécuritaire du projet et réalise une projection stratégique en tenant compte des risques, des évolutions législatives et évolutions des bonnes pratiques.
Périodicité	Selon les modalités convenues entre les Parties.
Ordre du jour	• Stratégie Sécurité des deux Parties • Revue du PAS • Revue des évolutions normatives et législatives • Relevé des décisions et actions à engager
Durée	Selon actualité
Participants à minima	• RSMOA • RSMOE
Animation / Rédaction du CR	Animation : RSMOE Rédaction : RSMOE
Diffusion du RIDA	Il est diffusé aux participants ainsi qu'au comité de suivi pour prise en compte des actions sécurité à mener.

Validation du RIDA	Ce compte-rendu doit faire l'objet de remarques écrites ou être approuvé par les membres du comité de sécurité sous 10 jours ouvrés après remise. Sans remarque sous 10 jours ouvrés, le compte-rendu est considéré comme validé.

Le RSMOE pourra convier à ces réunions les intervenants impliqués dans les sujets inscrits à l'ordre du jour : sécurité applicative, sécurité des serveurs, sécurité des échanges, sécurité des données…

Il conseille le Client dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

6.2. Organisation de la maîtrise d'ouvrage :

Le Client désignera un interlocuteur « Responsable Sécurité Maitrise d'Ouvrage » (RSMOA). Le RSMOA sera responsable de l'ensemble de la sécurité du projet pour le Client tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec la Société.

Des réunions de pilotage sécurité seront organisées à la demande la Société ou du Client. Les participants à ces réunions seront le RSMOA, le RSMOE, ainsi que le responsable technique ou fonctionnel lorsqu'ils sont impliqués dans les points à l'ordre du jour.

La sécurité globale de notre cadre opérationnel, repose sur la participation active des différents intervenants : personnel interne qui avait un rôle dans le fonctionnement antérieur du système ou service faisant l'objet de la mise en place de sécurité [intégrateur, développeur, administrateur, exploitant, responsable technique, etc.], maîtrise d'ouvrage et maître d'œuvre.

Le RSMOA désigné par le Client a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement de la sécurité liée au projet : politique de sécurité interne du Client, documentation technique du système [documents d'ingénierie, documents d'exploitation, etc.], spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par la Société.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

- ✓ **Interlocuteurs spécifiques au projet côté Client**

Fonction	Description de la fonction
Représentant de la Direction Générale	Responsable de la maîtrise d'ouvrage globale du projet Rôle d'arbitre et de décisionnaire de la Maîtrise d'Ouvrage
RSMOA	Responsable de la maîtrise d'œuvre Signataire des procès-verbaux de recette Gestionnaire du projet global

7. Responsabilités liées au PAS

Les responsabilités liées au PAS, s'appliquent à l'ensemble des équipes : maîtrise d'œuvre (et aux sous-traitants éventuels) et maîtrise d'ouvrage.

Sa rédaction relève du RSMOE, il doit être approuvé par la maîtrise d'ouvrage ; sa bonne exécution est de la responsabilité la Société en tant que maître d'œuvre.

La cohérence de l'ensemble des mesures pourra être analysée et réévaluée lors des réunions d'avancement (ou revues de pilotage).

L'approbation formelle du PAS par le Client est préférable. Toutefois, si aucune remarque n'est parvenue au RSMOE avant le démarrage du projet, le PAS est considéré comme adopté par le RSMOA et donc le CLIENT.

8. Procédure d'évolution du PAS

Les mises à jour du PAS doivent être justifiées par une amélioration des conditions de déroulement du projet ou de la sécurité des fournitures. Toute évolution doit être référencée dans le suivi des versions.

Voici une liste non exhaustive des situations susceptibles d'entraîner une modification du PAS :

- Évolution du système d'information (configuration logicielle ou matérielle) ;
- Évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- Évolution du périmètre de l'opération.
- Évolution des obligations légales.

Le RSMOE est responsable de la rédaction du PAS initial et de ses évolutions.

Une révision du PAS pourra être réalisée en cas d'évolution du périmètre de l'opération ou des exigences de la maîtrise d'ouvrage, après accord de la maîtrise d'œuvre. Cette révision sera réalisée par le RSMOE. La version révisée du PAS sera transmise à la maîtrise d'ouvrage pour validation.

9. Diffusion du PAS

Une fois approuvé, le PAS est diffusé à tous les acteurs du projet.

Le RSMOE est responsable de la diffusion du PAS au sein de son organisation et auprès des sous-traitant éventuels.

Le RSMOA est responsable de la diffusion du PAS auprès de ses propres équipes et de ses autres intervenants le cas échéant (éditeur, intégrateur, auditeur, client final).

10. Applicabilité du PAS

Le PAS est applicable à l'ensemble des acteurs du projet.

Un acteur du projet identifiant un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement au RSMOE qui en avertira la maîtrise d'ouvrage. Le client devra remplir le formulaire de l'annexe ***non-respect***. Celui-ci sera annexé au PAS, spécifiant la forme de la demande, la cause, les impacts du non-respect ainsi que des propositions d'actions correctives.

Ce PAS liste l'ensemble des mesures techniques possibles. Il convient de se référer au contrat afin d'identifier les produits souscrits auprès la Société.

11. Non-application du PAS

Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès du RSMOE qui le portera à la connaissance du Client. Le Client devra remplir le formulaire de l'annexe ***demande de dérogation***. Celui-ci sera annexé au PAS, spécifiant la forme de la demande, les impacts et les mesures de sécurité proposées.

La non-application de dispositions du PAS est justifiée par une dérogation.

La non-application de dispositions du PAS non justifiée par une dérogation constitue un écart.

Un acteur du projet identifiant un écart doit en référer immédiatement auprès du RSMOE.

Le RSMOA et les responsables concernés sont notifiés, l'écart fera l'objet d'un point particulier lors du comité de pilotage suivant.

Les dispositions sont alors prises par le RSMOE avec l'appui du RSMOA pour :

- Faire respecter les procédures,
- Mener les actions correctives nécessaires pour lever l'écart,
- Faire évoluer le PAS,
- Établir ou faire établir une demande de dérogation.

12. Demande de dérogation

Un acteur du projet n'étant pas à même de remplir l'ensemble des clauses du PAS devra effectuer ***une demande de dérogation*** en remplissant le formulaire de l'annexe correspondant auprès du RSMOE qui le portera à la connaissance du Client.

La demande de dérogation de Sécurité du Système d'Information a un caractère exceptionnel et ponctuel ; elle est revue à la date de fin de dérogation ou à la demande du Client ou de la Société.

La dérogation peut concerner :

- Le non-respect d'une ou plusieurs dispositions définies et validées dans le PAS,
- Une demande de livraison d'un produit non conforme (exemple : livraison d'un lot de logiciels contenant des anomalies identifiées mais non clôturées).

La demande est étudiée et validée par les RSMOA et RSMOE.

Dans tous les cas, la demande et la décision sont enregistrées.

La durée de la dérogation autorisée sera précisée systématiquement. Une dérogation n'est jamais permanente et sera revue au moins annuellement.

13. Mesures de sécurité

La Société décline ci-dessous les différentes mesures de sécurité applicables dans le cadre de la gestion du système d'information du donneur d'ordres et de sa gestion pendant les différentes phases contractuelles.

13.1. Transfert

La Société se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système d'information.

Le Client est garant de l'exploitabilité de ses sauvegardes. Il réalisera et gérera ses sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système.

Les modalités sont précisées dans les annexes jointes liées aux types de contrats souscrits (Infogérance, Hébergement, Sûreté, Telecom).

13.2. Exploitation

➢ ***Authentification***

La Société préconise les mesures suivantes concernant l'utilisation de l'identification par mot de passe :

Il appartient au Client de modifier son mot de passe par défaut dès la première connexion et d'en choisir un nouveau qui soit exclusif et confidentiel.

Un mot de passe est individuel, confidentiel et incessible.

L'identifiant et le mot de passe valent preuve de l'identité du Client et l'engagent sur toute utilisation faite par son intermédiaire. Il est rappelé que le Client est seul responsable de son nom d'utilisateur et de son mot de passe, il relève de sa seule responsabilité d'assurer la confidentialité de ses éléments d'identification. Le Client supportera seul les conséquences qui pourraient résulter de l'utilisation par des tiers qui auraient eu connaissance de ceux-ci.

La Société ne divulguera pas et ne changera pas les mots de passe sans vérification de l'identité du Client, si besoin par demande écrite et signée du Client.

Un mot de passe fort est préconisé et doit satisfaire quelques contraintes :

- Avoir une longueur minimale de 12 caractères ;
- Comporter au minimum une majuscule, un chiffre et un caractère spécial ;
- Changement des mots de passe par stratégie ou manuelle tous les 4 Mois ;
- Ne pas mettre les 3 derniers mots de passe utilisés précédemment ;
- Etre renouvelé régulièrement (90 jours est un bon compromis) ;
- Eviter de réutiliser le même mot de passe pour un autre service ;
- Ne pas le stocker en clair, utiliser un logiciel chiffrant les informations.

➢ ***Confidentialité et intégrité des flux***

En ce qui concerne les protocoles de télémaintenance (ou prise en main à distance), la Société utilise un logiciel sécurisé de télémaintenance pour les connexions à la demande. La société ne s'autorise pas à se connecter chez le Client sans son autorisation expresse.

De ce fait, soit un code de session est demandé au Client avant la connexion, soit le Client se connecte à une URL le plaçant en file d'attente de traitement. Dans tous les cas, c'est le Client qui autorise la Société à se connecter sur son réseau.

Dans le cas où le Client ne souhaite pas être sollicité à chaque télémaintenance, pour une durée limitée ou pour la durée du contrat de service, la Société peut utiliser :

- Un logiciel sécurisé de télémaintenance dont une partie déjà installée et active sur un équipement client ne nécessite pas d'action du Client.
- Une connexion RDP dont l'accès est limité au VPN site à site pouvant être monté entre la Société et le Client, si celui-ci est techniquement réalisable.
- Une connexion RDP directe dont l'accès sera limité à nos IP sur le pare-feu Client.

Dans ce cas, le Client devra donner son autorisation explicite et formelle, soit en remplissant le formulaire de l'annexe « ***Demande d'accès distant temporaire ou permanent***, soit en indiquant son accord sur l'extranet Do'comm mis à sa disposition.

Tous ces accès sont nominatifs, journalisés et feront l'objet d'un compte rendu disponible à la demande par le Client.

Toute clé de chiffrement est une information sensible et donc critique. La Société préconise donc au Client de s'assurer de la conservation sécurisée de ces clés. En aucun cas, la Société ne pourra assumer sa conservation ni sa sauvegarde afin de préserver la confidentialité des données.

La Société, sur les recommandations de l'ANSSI, conseille de conserver ces informations dans un coffre-fort numérique.

Des mesures spécifiques peuvent être mises en œuvre en fonction du type de prestation assurée. Celles-ci sont précisées dans les annexes (PAS - Annexe « Infogérance », « MSP », « Sûreté », « Telecom Téléphonie », « Applications de gestion ») et permettent de répondre aux exigences de protection du système.

13.3. Confidentialité

Se reporter aux Conditions Générales de Vente concernant cette clause de confidentialité. Un accord spécifique pour les projets sensibles peut être mis en place en remplissant le formulaire de l'annexe « ***Clause de confidentialité*** ». Ce formulaire doit être rédigé conjointement entre la Société et le Client, voire le(s) intervenant(s) nommé(s) des deux Parties.

13.4. Convention de service

Cette clause est la formalisation d'un accord entre la Société et le Client relatif au niveau de service attendu. Nos engagements, s'il y en a, sont spécifiés dans les Conditions Particulières et/ou Conditions Spécifiques liées aux types de Service souscrits.

Ces engagements pourront être définis pendant une phase probatoire, et réajustés à l'issue de celle-ci. Ils pourront également être redéfinis en cas de modification du périmètre de l'opération.

13.5. Audits de sécurité

Le Client pourra, à tout moment, contrôler que les exigences de sécurité sont satisfaites par les dispositions prises par la Société.

Le périmètre et la périodicité des audits de sécurité doivent être précisément définis.

Les audits pourront être réalisés par le Client, ou délégués à un tiers non concurrent de la Société. Le contrôle s'effectuera selon des modalités contractuelles définies Il est entendu que cet audit ne doit pas avoir pour conséquence de perturber l'exploitation du service de la Société.

La sécurité du Système d'Information de la Société et de ces Datacenter reposant sur leur accès restreint, le périmètre d'un audit sur site sera limité aux processus de la Société concernés par le traitement de Données à Caractère Personnel.

Cette visite sera notifiée à la Société selon un délai de Vingt (20) jours leur permettant d'organiser l'audit de sécurité.

En cas d'une intervention urgente, cas de la survenance d'un incident de sécurité, la Société mettra tout en œuvre pour apporter une réponse au Client.

La pratique de tests intrusifs doit être encadrée par une charte commune signée entre la Société, l'exécutant de l'audit et le Client.

Si le Client doit avoir recours à l'expertise d'un organisme ou d'une société tierce, la Société se réserve le droit de demander des justificatifs au Client afin de s'assurer des compétences de l'organisme ou de la société tierce en matière de sécurité.

13.6. Réversibilité

La clause de réversibilité est spécifiée dans les Conditions Particulières et/ou dans les Conditions Spécifiques liées aux types de Service souscrits.