Exigences de sécurité – Prestations de service

Définitions

Bien(s) D'EPSA MARKETPLACE : tout (i) élément logique, notamment fichier, données reçues et traitées et supprimées et/ou données du Client (à l'exception des Données personnelles du Client) incorporés dans les Services ou (ii) bien tangible appartenant au Client (y compris les livrables) utilisé, transformé et/ou transféré pour la réalisation des Services.

Incident de Sécurité : atteinte à la sécurité qui entraîne une menace concrète ou imminente d'un accès, d'une utilisation, d'une divulgation, d'une infraction, d'une modification, d'un vol, d'une perte, d'une corruption/d'une altération ou d'une destruction non autorisé(e) ou illégal(e) d'un Bien D'EPSA MARKETPLACE / de Données personnelles du Client, d'une interférence avec des opérations informatiques ou d'une interférence avec le fonctionnement du système. Ceci couvre, notamment, la perte ou le vol de dispositifs mobiles, des dysfonctionnements, une coupure d'alimentation, des surcharges, des erreurs commises par les utilisateurs/le personnel du système informatique, des violations d'accès, des programmes malveillants, du piratage.

Politique de Sécurité: les conditions de sécurité pour un système et/ou une organisation.

- Pour une organisation, les exigences physiques de sécurité telles que portes, des verrous, des clés et des murs ;
- Pour des systèmes, les contraintes imposées aux fonctions et aux flux entre ces dernières et les contraintes imposées à l'accès par des systèmes extérieurs, notamment par des programmes et à l'accès aux données par des personnes physiques.

Services sur site : Services fournis par un Fournisseur travaillant sur un site du Client ou du propre client du Client et qui accède au système informatique du Client ou de son propre client.

Services hors site connectés au système informatique du Client: Services fournis par un Fournisseur à partir du site du Fournisseur, qui accède au système informatique du Client ou du client du Client:

- soit dans un espace dédié et sécurisé réservé au Client uniquement ;
- soit à partir de ses locaux, en conformité avec les règles de sécurité EPSA MARKETPLACE.

Services hors site non connectés au système informatique du Client: Services fournis par un Fournisseur à partir du site du Fournisseur, sans accéder au système informatique du Client ou du client du Client.

Politique de Sécurité

Le Fournisseur garantit qu'il a développé, mis en œuvre une Politique de Sécurité complète et écrite et qu'il la mettra à jour et contrôlera son application, contenant des exigences de sécurité concernant les sites, les activités, le personnel et les systèmes utilisés pour développer, exécuter et livrer les Services (par exemple ISO 27001, NIST).

Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Le Fournisseur notifiera le Client dans un délai d'un (1) mois de toute mise à jour de sa Politique de Sécurité. Dans tous les cas, le Fournisseur ne saurait diminuer le niveau de sécurité des Services.

b. Le Client peut réviser les politiques et procédures de sécurité sur le site du Fournisseur, qui peuvent avoir une incidence sur la réalisation des Services.

Le Fournisseur respectera la dernière version de la Protection des Informations D'EPSA MARKETPLACE telles que communiquées par le Client, applicables aux produit, services et aux technologies informatiques livrés dans le cadre de l'exécution des Services ou nécessaires à la réalisation des Services.

Organisation de la sécurité des informations

Avant l'exécution des Services, le Fournisseur communiquera au Client ses règles de gouvernance concernant la sécurité et la cybersécurité, notamment les points de contact ainsi que leurs responsabilités et tâches.

Sécurité des Ressources Humaines

Lorsque le Fournisseur réalise un travail sur le site du Client ou sur le site du client du Client, il respectera les règles de sécurité physique et logique internes ainsi que les réglementations applicables à de tels sites, et reconnaît ses responsabilités en ce qui concerne la sécurité ainsi que les conséquences en cas de non-respect des règles de sécurité.

Gestion des Biens D'EPSA MARKETPLACE / des Données personnelles du Client

Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Le Fournisseur établira et maintiendra des protections administratives, techniques et physiques afin de protéger la sécurité, l'intégrité, la confidentialité et la disponibilité des Biens D'EPSA MARKETPLACE et des Données personnelles du Client et, notamment pour protéger les Biens D'EPSA MARKETPLACE et les Données personnelles du Client contre toute menace, danger anticipé et les protéger contre tout Incident de Sécurité.

b. Le Fournisseur tient un inventaire de tous les Biens D'EPSA MARKETPLACE (ou des composants qui supportent ces Biens).

Contrôle d'accès

Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Les administrateurs du Fournisseur assument la pleine responsabilité d'accorder l'accès aux Biens D'EPSA MARKETPLACE et aux Données personnelles du Client à tous les employés du Fournisseur et aux autres utilisateurs, et de fournir un processus qui gèrera la création et la suppression d'une manière sûre et dans les délais des comptes des employés et des autres comptes des utilisateurs. Ce processus doit comporter un accord approprié de la direction, un historique vérifiable de tous les changements et une révision annuelle de l'autorisation d'accès et d'une réhabilitation des accès excessifs. Le Fournisseur établira, maintiendra et appliquera les

principes d'accès de sécurité de la « ségrégation des tâches » et de « double vérification (Dual Control) » et du « moindre privilège » en ce qui concerne les Biens D'EPSA MARKETPLACE et les Données personnelles du Client.

b. Le Fournisseur enregistrera et conservera les journaux de tous les accès aux Biens d'EPSA MARKETPLACE, aux Données personnelles du Client et au système informatique du Client par son personnel, ses agents ou sous-traitants et ces journaux seront communiqués au Client. Dans le cas de Services exécutés hors site Client connectés au système informatique d'EPSA MARKETPLACE, le Fournisseur soumet à l'approbation du Client l'identité de tout employé du Fournisseur qui se verra accorder les privilèges d'accès à distance aux systèmes informatiques et aux réseaux du Client hébergés sur le site du Client. Ceci s'applique en particulier lorsque l'opération implique de créer un compte pour une personne qui figure sur le répertoire du Client.

Sécurité physique et environnementale

Si le Fournisseur fournit des Services au Client à partir de ses locaux, il respectera le Plan de Prévention communiqué par le Client dans la mesure où il serait applicable aux services et aux technologies informatiques livrés dans le cadre de l'exécution des Services ou nécessaires à la réalisation des Services. Dans le cas de Services exécutés hors site Client connectés au système informatique d'EPSA MARKETPLACE, le Fournisseur indiquera les emplacements géographiques dans lesquels il exploite les Biens D'EPSA MARKETPLACE et /ou traite les Données personnelles du Client. Notamment, le Fournisseur fournira l'adresse de :

a. son centre de données primaire et/ou de l'installation informatique et,

b. de son site de sauvegarde et/ou de reprise après sinistre.

Sécurité des opérations

Le Fournisseur maintiendra un environnement de sécurité conçu pour s'assurer que les Services sont protégés contre les programmes malveillants. Notamment, le Fournisseur :

a. prendra toutes les précautions et utilisera tous les moyens disponibles pour prévenir l'intrusion de codes malveillants sur ses serveurs, postes de travail et sur toute l'infrastructure éventuelle (par exemple, passerelle de courrier électronique, etc.);

b. mettra en œuvre des contrôles de détection, de prévention et de récupération pour protéger ses systèmes contre les programmes malveillants. Des mesures de quarantaine applicables seront mises en place sur les dispositifs de réseau infectés jusqu'à ce qu'ils soient nettoyés ;

c. veillera à ce que des moteurs logiciels antivirus/anti-intrusion et leurs modèles/bases de données de signatures soient mis à jour régulièrement sur tous les dispositifs, y compris sur les dispositifs mobiles. Le Fournisseur veillera à ce que des correctifs critiques soient appliqués à ses systèmes conformément à ce qui est recommandé par les fournisseurs de logiciels et après que le Fournisseur ait testé leur comptabilité avec ses installations. Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Le Fournisseur s'engage à employer des logiciels supportés commercialement (par exemple, logiciel sous maintenance active, y compris système d'exploitation, logiciel libre ou logiciel d'application et/ou similaire) sur tous systèmes qui traitent, stockent ou supportent techniquement les Services.

b. Le Fournisseur notifiera le Client un (1) an avant toute fin de support commercial de tout composant.

Acquisition, développement et maintenance des systèmes

Règles pour le développement des logiciels et des systèmes qui seront définies et appliquées aux développements à l'intérieur de l'organisation. Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client), les règles pour le développement des logiciels incluront au minimum :

a. pas d'utilisation d'identifiants codés en dur ;

b. séparation des rôles d'administrateurs et d'utilisateur ;

c. suppression systématique de tous les comptes par défaut utilisés dans le processus de développement et modification du mot de passe par défaut avant la livraison au Client. Le Fournisseur apportera des preuves sur les points suivants concernant la réalisation des Services :

a. les cyber-risques auxquels sont exposés les Services seront identifiés et entraîneront la création de contrôles de cybersécurité appropriés à mettre en place ;

b. les sources de données fiables et non fiables seront identifiées (par exemple, les sources de données internes à l'organisation du Client peuvent être considérées comme fiables tandis que d'autres sources de données peuvent être considérées comme non fiables). Le Fournisseur s'engage à réaliser (au moins tous les ans) une évaluation de vulnérabilité de ses systèmes accédant à ou contenant des Biens D'EPSA MARKETPLACE et/ou des données personnelles du Client et atténuera les risques ou remédiera aux défauts critiques dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation. Le Fournisseur s'engage à fournir au Client les rapports précisant la date de l'évaluation, l'identité des personnes ayant réalisé l'évaluation et une indication du risque relatif aux vulnérabilités identifiées ainsi que le délai nécessaire pour y remédier. L'évaluation de la menace de vulnérabilité sera réalisée en utilisant des outils et/ou services correspondant aux standards du secteur. Le Fournisseur mettra en place un processus de contrôle des modifications techniques pour les produits logiciels et matériels.

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant toute livraison de livrable et fournira au Client un rapport sur la détection de ces programmes malveillants.

Dans le cas de Services exécutés sur site Client:

a. Le Fournisseur assurera une révision et un contrôle annuels de la fiabilité de la sécurité du système. Pour ce faire, le Fournisseur procédera à des examens périodiques de la sécurité de son réseau et de l'adéquation de sa Politique de Sécurité par rapport aux normes de sécurité du secteur et à ses procédures. Le Fournisseur évaluera régulièrement la sécurité de son réseau et des services associés afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour répondre aux nouveaux risques en matière de sécurité ou aux conclusions générées par les évaluations périodiques. Le Fournisseur identifiera, initiera, gérera, enregistrera, signalera et mettra en place toutes les mesures de remédiation/correction appropriées relatives à tout défaut identifié

par tout audit, évaluation, activité de surveillance ou Incident de Sécurité, dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation.

b. Le Client se réserve le droit d'interrompre ou de limiter la connectivité ou l'accès aux informations du Fournisseur dans les cas suivants :

- le Fournisseur refuse au Client la possibilité de réaliser un audit de sécurité ;
- des mesures de correction ne sont pas mises en place ; ou
- l'absence de collaboration en cas d'Incident de Sécurité majeur.

Gestion des Incidents de Sécurité

Le Fournisseur mettra en place un processus de gestion approfondi et agréé des Incidents de Sécurité pour les réseaux et les systèmes qu'il exploite, comprenant l'identification, la réponse, le confinement, la récupération, la signalisation, la protection des preuves et l'examen des Incidents de Sécurité ;. Le Fournisseur s'engage à informer le Client sans délai en cas d'événement, au plus tard vingt-quatre (24) heures après avoir eu connaissance d'un Incident de Sécurité, à l'adresse suivante : contact@epsa-marketplace.com. La notification devra inclure, à minima :

a. une déclaration ou une description du problème ;

b. le délai de remédiation attendu (si connu) ;

c. le nom et le numéro de téléphone du représentant du Fournisseur que le Client peut contacter pour obtenir des informations complémentaires. Les preuves liées à un Incident de Sécurité seront recueillies, conservées et présentées par le Fournisseur afin de respecter les règles de preuve applicables devant les juridictions compétentes.

Gestion de la continuité des opérations

Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Le Fournisseur aura déployé les moyens pour assurer la continuité commerciale et la reprise en cas de sinistre, y compris la résilience des Services livrés au Client ;

b. Le Fournisseur notifiera le Client en cas de sinistre.

Conformité

Dans le cas de Services exécutés hors site Client (connectés ou non au système informatique du Client) :

a. Le Fournisseur reconnaît que le Client ou un auditeur indépendant désigné par le Client peut, à ses propres frais, effectuer un audit du respect des engagements de sécurité du Fournisseur sur ses systèmes, processus et procédures et de sa chaîne logistique, ayant une incidence sur les Services ou les systèmes du Client. Ceci comporte, notamment, la vérification de l'accord et du contrôle d'accès, le contrôle du flux d'information et des journaux d'audit. Le Fournisseur fournira toute la documentation et les justificatifs nécessaires.

b. En raison de la nature confidentielle et exclusive des opérations du Fournisseur, et afin de protéger l'intégrité et la sécurité de ces opérations et la nature partagée des systèmes qui peuvent être utilisés pour fournir les Services:

- les parties conviendront à l'avance de la portée des audits ;
- un préavis écrit d'au moins trente (30) jours avant la date prévue de démarrage de l'audit sera donné par le Client et l'audit se produira au maximum une fois par période de douze (12) mois, à moins de circonstances telles que qu'une présomption raisonnable du Client d' Incident de Sécurité; dans ce cas, un audit pourra être réalisé à une date fixée d'un commun accord entre les parties ;
- si l'audit est réalisé par un tiers, ce dernier sera un auditeur expert e, sécurité et agréé par les parties, étant entendu que le Fournisseur ne pourra refuser le tiers auditeur sans motif légitime ;
- l'audit sera conduit conformément aux exigences et contraintes en matière de confidentialité et de non divulgation des parties; et
- l'audit ne saurait perturber de manière non raisonnable l'activité normale du Fournisseur ou ses opérations informatiques.

c. Nonobstant les dispositions, ci-dessus, le Client conserve le pouvoir discrétionnaire d'engager une inspection de sécurité au titre de la présente section, et il pourra initier l'inspection avant la réalisation des Services puis, (i) en cas de tout modification dans la réalisation des Services qui pourrait en affecter la sécurité, (ii) à la suite de tout Incident de Sécurité affectant les Services ou les Biens D'EPSA MARKETPLACE ou les Données personnelles du Client, et (iii) en cas de demande du Client ou de demande émanant d'un organisme gouvernemental. Le Fournisseur apportera au Client l'assistance raisonnable éventuellement nécessaire pour permettre au Client de respecter les lois applicables en matière de sécurité.

Le Fournisseur conservera et protégera tout preuve du respect des obligations légales ou contractuelles et seront mises à la disposition du Client si besoin

Exigences de sécurité - Produits sur étagère

Définitions

Incident de Sécurité : atteinte à la sécurité qui entraîne une menace concrète ou imminente d'un accès, d'une utilisation, d'une divulgation, d'une infraction, d'une modification, d'un vol, d'une perte, d'une corruption/d'une altération ou d'une destruction non autorisée(e) ou illégal(e) d'un Bien D'EPSA MARKETPLACE / de Données personnelles du Client, d'une interférence avec des opérations informatiques ou d'une interférence avec le fonctionnement du système. Ceci couvre, notamment, la perte ou le vol de dispositifs mobiles, des dysfonctionnements, une coupure d'alimentation, des surcharges, des erreurs commises par les utilisateurs/le personnel du système informatique, des violations d'accès, des programmes malveillants, du piratage.

Politique de Sécurité : les conditions de sécurité pour un système et/ou une organisation ;

- Pour une organisation, les exigences physiques de sécurité telles que portes, des verrous, des clés et des murs ;
- Pour des systèmes, les contraintes imposées aux fonctions et aux flux entre ces dernières et les contraintes imposées à l'accès par des systèmes extérieurs, notamment par des programmes et à l'accès aux données par des personnes physiques.

Organisation de la sécurité des informations

Avant la livraison des Produits, le Fournisseur communiquera au Client ses règles de gouvernance concernant la sécurité et la cybersécurité, notamment les points de contact et leurs responsabilités et tâches.

Sécurité des opérations

Le Fournisseur maintiendra un environnement de sécurité conçu pour s'assurer que les Produits ou services associés aux Produits sont protégés contre les programmes malveillants. Notamment, le Fournisseur :

a. prendra toutes les précautions et utilisera tous les moyens disponibles pour prévenir l'intrusion de codes malveillants sur ses serveurs, postes de travail et sur toute l'infrastructure éventuelle (par exemple, passerelle de courrier électronique, etc.);

b. mettra en œuvre des contrôles de détection, de prévention et de récupération pour protéger ses systèmes contre les programmes malveillants. Des mesures de quarantaine applicables seront mises en place sur les dispositifs de réseau infectés jusqu'à ce qu'ils soient nettoyés ;

c. veillera à ce que des moteurs logiciels antivirus/anti-intrusion et leurs modèles/bases de données de signatures soient mis à jour régulièrement sur tous les dispositifs, y compris sur les dispositifs mobiles.

Le Fournisseur veillera à ce que des correctifs critiques soient appliqués à ses systèmes conformément à ce qui est recommandé par les fournisseurs de logiciels et après que le Fournisseur ait testé leur comptabilité avec ses installations.

Acquisition, développement et maintenance des systems.

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant toute livraison de Produit et fournira au Client un rapport sur la détection de ces programmes malveillants.

Le Fournisseur assurera une révision et un contrôle annuels de la fiabilité de la sécurité du système. Pour ce faire, le Fournisseur procédera à des examens périodiques de la sécurité de son réseau et de l'adéquation de sa Politique de Sécurité par rapport aux normes de sécurité du secteur et à ses procédures. Le Fournisseur évaluera régulièrement la sécurité de son réseau et des services associés afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour répondre aux nouveaux risques en matière de sécurité ou aux conclusions générées par les évaluations périodiques. Le Fournisseur identifiera, initiera, gérera, enregistrera, signalera et mettra en place toutes les mesures de remédiation/correction appropriées relatives à tout défaut identifié par tout audit, évaluation, activité de surveillance ou Incident de Sécurité, dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation.

Le Client se réserve le droit d'interrompre ou de limiter la connectivité ou l'accès aux informations du Fournisseur dans les cas suivants :

- le Fournisseur refuse au Client la possibilité de réaliser un audit de sécurité ;
- des mesures de correction ne sont pas mises en place ; ou
- l'absence de collaboration en cas d'Incident de Sécurité majeur.

Le Fournisseur mettra en place un processus de contrôle des modifications techniques pour les produits logiciels et matériels.

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant la livraison au Client et fournira au Client le rapport sur la détection de ces programmes malveillants.

Gestion des incidents de sécurité des informations

Le Fournisseur mettra en place un processus de gestion approfondi et agréé des Incidents de Sécurité pour les réseaux et les systèmes qu'il exploite, comprenant l'identification, la réponse, le confinement, la récupération, la signalisation, la protection des preuves et l'examen des Incidents de Sécurité. Le Fournisseur s'engage à informer le Client sans délai en cas d'événement, au plus tard vingt-quatre (24) heures après avoir eu connaissance d'un Incident de Sécurité, à l'adresse suivante : Contact@epsa-marketplace.com. La notification devra inclure, à minima :

a. une déclaration ou une description du problème ;

b. le délai de remédiation attendu (si connu) ;

c. le nom et le numéro de téléphone du représentant du Fournisseur que le Client peut contacter pour obtenir des informations complémentaires.

Les preuves liées à un Incident de Sécurité seront recueillies, conservées et présentées par le Fournisseur afin de respecter les règles de preuve applicables devant les juridictions compétentes.

Gestion de la continuité des opérations

Le Fournisseur aura déployé les moyens pour assurer la continuité commerciale et la reprise en cas de sinistre, y compris la résilience des Produits livrés au Client. Le Fournisseur notifiera le Client en cas de sinistre

Exigences de sécurité - Logiciels

Définitions

Bien(s) D'EPSA MARKETPLACE : tout (i) élément logique, notamment fichier, données reçues et traitées et supprimées et/ou données du Client (à l'exception des Données personnelles du Client) incorporés dans les Services ou (ii) bien tangible appartenant au Client (y compris les livrables) utilisé, transformé et/ou transféré pour la réalisation des Services.

Incident de Sécurité : atteinte à la sécurité qui entraîne une menace concrète ou imminente d'un accès, d'une utilisation, d'une divulgation, d'une infraction, d'une modification, d'un vol, d'une perte, d'une corruption/d'une altération ou d'une destruction non autorisé(e) ou illégal(e) d'un Bien D'EPSA MARKETPLACE / de Données personnelles du Client, d'une interférence avec des opérations informatiques ou d'une interférence avec le fonctionnement du système. Ceci couvre, notamment, la perte ou le vol de dispositifs mobiles, des dysfonctionnements, une coupure d'alimentation, des surcharges, des erreurs commises par les utilisateurs/le personnel du système informatique, des violations d'accès, des programmes malveillants, du piratage.

Politique de Sécurité : les conditions de sécurité pour un système et/ou une organisation ;

- pour une organisation, les exigences physiques de sécurité telles que portes, des verrous, des clés et des murs ;
- pour des systèmes, les contraintes imposées aux fonctions et aux flux entre ces dernières et les contraintes imposées à l'accès par des systèmes extérieurs, notamment par des programmes et à l'accès aux données par des personnes physiques.

Organisation de la sécurité des informations

Avant la livraison des Produits, le Fournisseur communiquera au Client ses règles de gouvernance concernant la sécurité et la cybersécurité, notamment les points de contact et leurs responsabilités et tâches.

Sécurité des opérations

Le Fournisseur maintiendra un environnement de sécurité conçu pour s'assurer que les Produits ou services associés aux Produits sont protégés contre les programmes malveillants. Notamment, le Fournisseur :

a. prendra toutes les précautions et utilisera tous les moyens disponibles pour prévenir l'intrusion de codes malveillants sur ses serveurs, postes de travail et sur toute l'infrastructure éventuelle (par exemple, passerelle de courrier électronique, etc.);

b. mettra en œuvre des contrôles de détection, de prévention et de récupération pour protéger ses systèmes contre les programmes malveillants. Des mesures de quarantaine applicables seront mises en place sur les dispositifs de réseau infectés jusqu'à ce qu'ils soient nettoyés ;

c. veillera à ce que des moteurs logiciels antivirus/anti-intrusion et leurs modèles/bases de données de signatures soient mis à jour régulièrement sur tous les dispositifs, y compris sur les dispositifs mobiles.

Le Fournisseur veillera à ce que des correctifs critiques soient appliqués à ses systèmes conformément à ce qui est recommandé par les fournisseurs de logiciels et après que le Fournisseur ait testé leur comptabilité avec ses installations.

Acquisition, développement et maintenance des systèmes

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant toute livraison de Produit et fournira au Client un rapport sur la détection de ces programmes malveillants.

Le Fournisseur assurera une révision et un contrôle annuels de la fiabilité de la sécurité du système. Pour ce faire, le Fournisseur procédera à des examens périodiques de la sécurité de son réseau et de l'adéquation de sa Politique de Sécurité par rapport aux normes de sécurité du secteur et à ses procédures. Le Fournisseur évaluera régulièrement la sécurité de son réseau et des services associés afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour répondre aux nouveaux risques en matière de sécurité ou aux conclusions générées par les évaluations périodiques. Le Fournisseur identifiera, initiera, gérera, enregistrera, signalera et mettra en place toutes les mesures de remédiation/correction appropriées relatives à tout défaut identifié par tout audit, évaluation, activité de surveillance ou Incident de Sécurité, dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation.

Le Client se réserve le droit d'interrompre ou de limiter la connectivité ou l'accès aux informations du Fournisseur dans les cas suivants :

- le Fournisseur refuse au Client la possibilité de réaliser un audit de sécurité ;
- des mesures de correction ne sont pas mises en place ; ou
- l'absence de collaboration en cas d'Incident de Sécurité majeur.

Le Fournisseur mettra en place un processus de contrôle des modifications techniques pour les produits logiciels et matériels.

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant la livraison au Client et fournira au Client le rapport sur la détection de ces programmes malveillants.

Gestion des Biens d'EPSA MARKETPLACE

Le service du Fournisseur est doté d'un dispositif de suppression automatique pour supprimer les données personnelles du Client à la fin de la période de conservation des données. Le Fournisseur apportera, sur demande, une assistance raisonnable au Client pour respecter toutes les lois et réglementations applicables aux Biens D'EPSA MARKETPLACE et aux données personnelles liées, notamment, à l'identification, à l'étiquetage, à la recherche, à la dépersonnalisation, à la signalisation, à la copie, à la modification, au transfert et à l'extraction. Le Fournisseur devra, dans ce cas, fournir au Client toutes les informations dont le Client peut avoir besoin ou qui peuvent s'avérer nécessaires.

Gestion des Incidents de Sécurité

Le Fournisseur mettra en place un processus de gestion approfondi et agréé des Incidents de Sécurité pour les réseaux et les systèmes qu'il

exploite, comprenant l'identification, la réponse, le confinement, la récupération, la signalisation, la protection des preuves et l'examen des Incidents de Sécurité. Le Fournisseur s'engage à informer le Client sans délai en cas d'événement, au plus tard vingt-quatre (24) heures après avoir eu connaissance d'un Incident de Sécurité, à l'adresse suivante : Contact@epsa-marketplace.com. La notification devra inclure, à minima :

a. une déclaration ou une description du problème ;

b. le délai de remédiation attendu (si connu) ;

c. le nom et le numéro de téléphone du représentant du Fournisseur que le Client peut contacter pour obtenir des informations complémentaires. Les preuves liées à un Incident de Sécurité seront recueillies, conservées et présentées par le Fournisseur afin de respecter les règles de preuve applicables devant les juridictions compétentes.

Gestion de la continuité des opérations

Le Fournisseur aura déployé les moyens pour assurer la continuité commerciale et la reprise en cas de sinistre, y compris la résilience des Produits livrés au Client. Le Fournisseur notifiera le Client en cas de sinistre.

Exigences de sécurité – Matériel fabriqué sur mesure/construit selon spécifications

Définitions

Bien(s) D'EPSA MARKETPLACE : tout (i) élément logique, notamment fichier, données reçues et traitées et supprimées et/ou données du Client (à l'exception des Données personnelles du Client) incorporés dans les Services ou (ii) bien tangible appartenant au Client (y compris les livrables) utilisé, transformé et/ou transféré pour la réalisation des Services.

Incident de Sécurité : atteinte à la sécurité qui entraîne une menace concrète ou imminente d'un accès, d'une utilisation, d'une divulgation, d'une infraction, d'une modification, d'un vol, d'une perte, d'une corruption/d'une altération ou d'une destruction non autorisé(e) ou illégal(e) d'un Bien D'EPSA MARKETPLACE / de Données personnelles du Client, d'une interférence avec des opérations informatiques ou d'une interférence avec le fonctionnement du système. Ceci couvre, notamment, la perte ou le vol de dispositifs mobiles, des dysfonctionnements, une coupure d'alimentation, des surcharges, des erreurs commises par les utilisateurs/le personnel du système informatique, des violations d'accès, des programmes malveillants, du piratage.

Politique de Sécurité : les conditions de sécurité pour un système et/ou une organisation ;

- pour une organisation, les exigences physiques de sécurité telles que portes, des verrous, des clés et des murs ;
- pour des systèmes, les contraintes imposées aux fonctions et aux flux entre ces dernières et les contraintes imposées à l'accès par des systèmes extérieurs, notamment par des programmes et à l'accès aux données par des personnes physiques.

Politique de Sécurité

Le Fournisseur garantit qu'il a développé, mis en œuvre une Politique de Sécurité complète et écrite et qu'il la mettra à jour et contrôlera son application, contenant des exigences de sécurité concernant les sites, les activités, le personnel et les systèmes utilisés pour développer, réaliser et livrer les Produits (par exemple ISO 27001, NIST).

Le Fournisseur notifiera le Client dans un délai d'un (1) mois de toute mise à jour de sa Politique de Sécurité. Dans tous les cas, le Fournisseur ne saurait diminuer le niveau de sécurité des Produits. Le Client peut réviser les politiques et procédures de sécurité sur le site du Fournisseur, qui peuvent avoir une incidence sur la fourniture des Produits.

Le Fournisseur respectera la dernière version de la Protection des Informations Groupe D'EPSA MARKETPLACE telles que communiquées par le Client, applicables aux produit, services et aux technologies informatiques nécessaires à la réalisation et livraison des Produits.

Organisation de la sécurité des informations

Avant la livraison des Produits, le Fournisseur communiquera au Client ses règles de gouvernance concernant la sécurité et la cybersécurité, notamment les points de contact et leurs responsabilités et tâches.

Sécurité des opérations

Le Fournisseur maintiendra un environnement de sécurité conçu pour s'assurer que les Produits sont protégés contre les programmes malveillants. Notamment, le Fournisseur :

a. prendra toutes les précautions et utilisera tous les moyens disponibles pour prévenir l'intrusion de codes malveillants sur ses serveurs, postes de travail et sur toute l'infrastructure éventuelle (par exemple, passerelle de courrier électronique, etc.);

b. mettra en œuvre des contrôles de détection, de prévention et de récupération pour protéger ses systèmes contre les programmes malveillants. Des mesures de quarantaine applicables seront mises en place sur les dispositifs de réseau infectés jusqu'à ce qu'ils soient nettoyés ;

c. veillera à ce que des moteurs logiciels antivirus/anti-intrusion et leurs modèles/bases de données de signatures soient mis à jour régulièrement sur tous les dispositifs, y compris sur les dispositifs mobiles.

Le Fournisseur s'engage à employer des logiciels supportés commercialement (par exemple, logiciel sous maintenance active, y compris système d'exploitation, logiciel libre ou logiciel d'application et/ou similaire) sur tous systèmes qui traitent, stockent ou supportent techniquement les Services. Le Fournisseur notifiera le Client un (1) an avant toute fin de support commercial de tout composant. Le Fournisseur veillera à ce que des correctifs critiques soient appliqués à ses systèmes conformément à ce qui est recommandé par les fournisseurs de logiciels et après que le Fournisseur ait testé leur comptabilité avec ses installations.

Le Fournisseur s'engage à employer des logiciels pris en charge supportés commercialement (par exemple, logiciel sous maintenance active, y compris système d'exploitation, logiciel libre ou logiciel d'application et/ou similaire) sur tous systèmes qui traitent, stockent ou supportent techniquement la fabrication des Produits.

Le Fournisseur notifiera le Client à l'avance un (1) an de toute fin de support commercial de tout composant.

Gestion des Biens D'EPSA MARKETPLACE / des Données personnelles du Client

Les Biens D'EPSA MARKETPLACE restent, à tout moment, la propriété exclusive du Client. Le Client se réserve le droit de demander au Fournisseur de modifier en toute diligence, de mettre à jour, de détruire et de retourner tout Bien d'EPSA MARKETPLACE, de toute manière, qui se trouve sous la responsabilité du Fournisseur. Le Fournisseur sera en mesure, à la demande du Client, de retourner et/ou de supprimer les Données personnelles du Client au plus tard un (1) mois après la demande du Client.

Le Fournisseur établira et maintiendra des protections administratives, techniques et physiques afin de protéger la sécurité, l'intégrité, la confidentialité et la disponibilité des Biens D'EPSA MARKETPLACE et des Données personnelles du Client et, notamment pour protéger les Biens D'EPSA MARKETPLACE et les Données personnelles du Client contre toute menace, danger anticipé et les protéger contre tout Incident de Sécurité. Le Fournisseur tient un inventaire de tous les

Biens D'EPSA MARKETPLACE (ou des composants qui supportent ces Biens)

Les Biens D'EPSA MARKETPLACE ou toute partie de ces derniers ne sauraient être retenus, d'une quelconque manière, au-delà de la durée de livraison des Produits, sauf conformément à ce qui est exigé par la loi ou par le Client.

Si le Fournisseur désire modifier sensiblement le processus, la méthode ou les moyens d'utilisation, de divulgation, de stockage, de traitement ou de transmission ou de gestion des Biens EPSA MARKETPLACE, le Fournisseur préviendra le Client par un préavis écrit d'au moins quatre-vingt-dix (90) jours. Le Client sera en droit, à son entière discrétion, de déterminer si les modifications représentent des risques inacceptables et pourra interdire au Fournisseur la mise en œuvre de toute modification de ce type sur les Produits jusqu'à ce que les risques puissent être atténués ou qu'une autre source puisse être trouvée pour les Produits.

Le service du Fournisseur est doté d'un dispositif de suppression automatique pour supprimer les Données personnelles du Client à la fin de la période de conservation des données.

Le Fournisseur apportera, sur demande, une assistance raisonnable au Client pour respecter toutes les lois et réglementations applicables aux Biens D'EPSA MARKETPLACE et aux Données personnelles du Client liées, notamment, à l'identification, à l'étiquetage, à la recherche, à la dépersonnalisation, à la signalisation, à la copie, à la modification, au transfert et à l'extraction. Le Fournisseur devra, dans ce cas, fournir au Client toutes les informations dont le Client peut avoir besoin ou qui peuvent s'avérer nécessaires.

Contrôle d'acces

Les administrateurs du Fournisseur assument la pleine responsabilité d'accorder l'accès aux Biens D'EPSA MARKETPLACE et aux Données personnelles du Client à tous les employés du Fournisseur et aux autres utilisateurs, et de fournir un processus qui gèrera la création et la suppression d'une manière sûre et dans les délais des comptes des employés et des autres comptes des utilisateurs. Ce processus doit comporter un accord approprié de la direction, un historique vérifiable de tous les changements et une révision annuelle de l'autorisation d'accès et d'une réhabilitation des accès excessifs. Le Fournisseur établira, maintiendra et appliquera les principes d'accès de sécurité de la « ségrégation des tâches » et de « double vérification (Dual Control) » et du « moindre privilège » en ce qui concerne les Biens D'EPSA MARKETPLACE et les Données personnelles du Client.

Le Fournisseur enregistrera et conservera les journaux de tous les accès aux Biens EPSA MARKETPLACE, aux données personnelles du Client et au système informatique du Client par son personnel, ses agents ou soustraitants et ces journaux seront communiqués au Client.

Acquisition, développement et maintenance des systèmes

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant toute livraison de Livrable et fournira au Client un rapport sur la détection de ces programmes malveillants.

Les règles pour le développement des logiciels incluront au minimum:

a. pas d'utilisation d'identifiants codés en dur ;

b. séparation des rôles d'administrateurs et d'utilisateur ;

c. suppression systématique de tous les comptes par défaut utilisés dans le processus de développement et modification du mot de passe par défaut avant la livraison au Client. Le Fournisseur apportera des preuves sur les points suivants concernant la conception des Produits: a. les cyber-risques auxquels sont confrontés exposés les Produits seront identifiés et entraîneront la création de contrôles de cybersécurité appropriés à mettre en place ;

d. les sources de données fiables et non fiables seront identifiées (par exemple, les sources de données internes à l'organisation du Client peuvent être considérées comme fiables tandis que d'autres sources de données peuvent être considérées comme non fiables).

Le Fournisseur s'engage à réaliser (au moins tous les ans) une évaluation de vulnérabilité de ses systèmes accédant à ou contenant des Biens D'EPSA MARKETPLACE et/ou des Données personnelles du Client et atténuera les risques ou remédiera aux défauts critiques dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation. Le Fournisseur s'engage à fournir au Client les rapports précisant la date de l'évaluation, l'identité des personnes ayant réalisé l'évaluation et une indication du risque relatif aux vulnérabilités identifiées ainsi que le délai nécessaire pour y remédier. L'évaluation de la menace de vulnérabilité sera réalisée en utilisant des outils et/ou services correspondant aux standards du secteur.

Le Fournisseur mettra en place un processus de contrôle des modifications techniques pour les produits logiciels et matériels.

Gestion de la continuité des opérations

Le Fournisseur aura déployé les moyens pour assurer la continuité commerciale et la reprise en cas de sinistre, y compris la résilience des Produits livrés au Client. Le Fournisseur notifiera le Client en cas de sinistre.

Gestion des Incidents de Sécurité

Le Fournisseur mettra en place un processus de gestion approfondi et agréé des Incidents de Sécurité pour les réseaux et les systèmes qu'il exploite, comprenant l'identification, la réponse, le confinement, la récupération, la signalisation, la protection des preuves et l'examen des Incidents de Sécurité. Le Fournisseur s'engage à informer le Client sans délai en cas d'événement, au plus tard vingt-quatre (24) heures après avoir eu connaissance d'un Incident de Sécurité, à l'adresse suivante : Contact@epsa-marketplace.com. La notification devra inclure, à minima :

a. une déclaration ou une description du problème ;

b. le délai de remédiation attendu (si connu) ;

c. le nom et le numéro de téléphone du représentant du Fournisseur que le Client peut contacter pour obtenir des informations complémentaires.

Les preuves liées à un Incident de Sécurité seront recueillies, conservées et présentées par le Fournisseur afin de respecter les règles de preuve applicables devant les juridictions compétentes.

Conformité

Le Fournisseur reconnaît que le Client ou un auditeur indépendant désigné par le Client peut, à ses propres frais, effectuer un audit du respect des engagements de sécurité du Fournisseur sur ses systèmes, processus et procédures et de sa chaîne logistique, ayant une incidence sur les Produits ou les systèmes du Client. Ceci comporte, notamment, la vérification de l'accord et du contrôle d'accès, le contrôle du flux d'information et des journaux d'audit. Le Fournisseur fournira toute la documentation et les justificatifs nécessaires.

En raison de la nature confidentielle et exclusive des opérations du Fournisseur, et afin de protéger l'intégrité et la sécurité de ces opérations et la nature partagée des systèmes qui peuvent être utilisés pour fournir les Produits:

- les parties conviendront à l'avance de la portée des audits ;
- un préavis écrit d'au moins trente (30) jours avant la date prévue de démarrage de l'audit sera donné par le Client et l'audit se produira au maximum une fois par période de douze (12) mois, à moins de circonstances telles que qu'une présomption raisonnable du Client d'Incident de Sécurité; dans ce cas, un audit pourra être réalisé à une date fixée d'un commun accord entre les parties ;
- si l'audit est réalisé par un tiers, ce dernier sera un auditeur expert en sécurité et agréé par les parties, étant entendu que le Fournisseur ne pourra refuser le tiers auditeur sans motif légitime ;
- l'audit sera conduit conformément aux exigences et contraintes en matière de confidentialité et de non divulgation des parties; et
- l'audit ne saurait perturber de manière non raisonnable l'activité normale du Fournisseur ou ses opérations informatiques.

Nonobstant les dispositions, ci-dessus, le Client conserve le pouvoir discrétionnaire d'engager une inspection de sécurité au titre de la présente section, et il pourra initier l'inspection avant la livraison des Produits puis, (i) en cas de tout modification dans la livraison des Produits qui pourrait en affecter la sécurité, (ii) à la suite de tout Incident de Sécurité affectant les Produits ou les Biens D'EPSA MARKETPLACE ou les données personnelles du Client, et (iii) en cas de demande du Client ou de demande émanant d'un organisme gouvernemental. Le Fournisseur apportera au Client l'assistance raisonnable éventuellement nécessaire pour permettre au Client de respecter les lois applicables en matière de sécurité.

Exigences de sécurité - SAAS

Définitions

Bien(s) D'EPSA MARKETPLACE : tout (i) élément logique, notamment fichier, données reçues et traitées et
supprimées et/ou données du Client (à l'exception des Données personnelles du Client) incorporés
dans les Services ou (ii) bien tangible appartenant au Client (y compris les livrables) utilisé, transformé et/ou transféré pour la réalisation des Services.

Incident de Sécurité : atteinte à la sécurité qui entraîne une menace concrète ou imminente d'un accès, d'une utilisation, d'une divulgation, d'une infraction, d'une modification, d'un vol, d'une perte, d'une corruption/d'une altération ou d'une destruction non autorisé(e) ou illégal(e) d'un Bien d'EPSA MARKETPLACE / de Données personnelles du Client, d'une interférence avec des opérations informatiques ou d'une interférence avec le fonctionnement du système. Ceci couvre, notamment, la perte ou le vol de
dispositifs mobiles, des dysfonctionnements, une coupure d'alimentation, des surcharges, des erreurs commises par les utilisateurs/le personnel du système informatique, des violations d'accès, des programmes malveillants, du piratage.

Politique de Sécurité : les conditions de sécurité pour un système et/ou une organisation ;

- pour une organisation, les exigences physiques de sécurité telles que portes, des verrous, des clés et des murs ;
- pour des systèmes, les contraintes imposées aux fonctions et aux flux entre ces dernières et les contraintes imposées à l'accès par des systèmes extérieurs, notamment par des programmes et à l'accès aux données par des personnes physiques.

Politique de Sécurité

Le Fournisseur garantit qu'il a développé, mis en œuvre une Politique de Sécurité complète et écrite et qu'il la mettra à jour et contrôlera son application, contenant des exigences de sécurité concernant les sites, les activités, le personnel et les systèmes utilisés pour développer, exécuter et livrer les Services/ Produits (par exemple ISO 27001, NIST).
Le Fournisseur notifiera le Client dans un délai d'un (1) mois de toute mise à jour de sa Politique de Sécurité. Dans tous les cas, le Fournisseur ne saurait diminuer le niveau de sécurité des Services/Produits.
Le Client peut réviser les politiques et procédures de sécurité sur le site du Fournisseur, qui peuvent avoir une incidence sur la réalisation des Services/fourniture des Produits.
Le Fournisseur respectera la dernière version de la Protection des Informations Groupe EPSA MARKETPLACE telles que communiquées par le Client, applicables aux produit, services et aux technologies informatiques livrés dans le cadre de l'exécution des Services ou nécessaires à la réalisation des Services.

Organisation de la sécurité des informations

Avant l'exécution des Services/l'exécution de la Commande, le Fournisseur/le Fournisseur
communiquera au Client ses règles de gouvernance concernant la sécurité et la cybersécurité,
notamment les points de contact ainsi que leurs responsabilités et tâches

Sécurité des Ressources Humaines

Le Fournisseur, doit s'assurer que son personnel est dûment formé aux obligations qui lui incombent lors du traitement de données personnelles du Client.

Gestion des Biens D'EPSA MARKETPLACE / des Données personnelles du Client

Les Biens D'EPSA MARKETPLACE restent, à tout moment, la propriété exclusive du Client. Le Client se réserve le
droit de demander au Fournisseur de modifier en toute diligence, de mettre à jour, de détruire et de
retourner tout Bien EPSA MARKETPLACE, de toute manière, qui se trouve sous la responsabilité du Fournisseur.

Le Fournisseur sera en mesure, à la demande du Client, de retourner et/ou de supprimer les Données personnelles du Client au plus tard un (1) mois après la demande du Client.

Le service du Fournisseur est doté d'un dispositif de suppression automatique pour supprimer les

Données personnelles du Client à la fin de la période de conservation des données.

Le Fournisseur établira et maintiendra des protections administratives, techniques et physiques afin
de protéger la sécurité, l'intégrité, la confidentialité et la disponibilité des Biens D'EPSA MARKETPLACE et des
Données personnelles du Client et, notamment pour protéger les Biens D'EPSA MARKETPLACE et les Données personnelles du Client contre toute menace, danger anticipé et les protéger contre tout Incident de Sécurité.

Le Fournisseur tient un inventaire de tous les Biens D'EPSA MARKETPLACE (ou des composants qui supportent ces Biens).

Le Fournisseur apportera, sur demande, une assistance raisonnable au Client pour respecter toutes les lois et réglementations applicables aux Biens D'EPSA MARKETPLACE et aux Données personnelles du Client liées, notamment, à l'identification, à l'étiquetage, à la recherche, à la dépersonnalisation, à la signalisation, à la copie, à la modification, au transfert et à l'extraction. Le Fournisseur devra, dans ce cas, fournir au Client toutes les informations dont le Client peut avoir besoin ou qui peuvent s'avérer nécessaires.

Contrôle d'accès

Les administrateurs du Fournisseur assument la pleine responsabilité d'accorder l'accès aux Biens D'EPSA MARKETPLACE et aux Données personnelles du Client à tous les employés du Fournisseur et aux autres utilisateurs, et de fournir un processus qui gèrera la création et la suppression d'une manière sûre et dans les délais des comptes des employés et des autres comptes des utilisateurs. Ce processus doit comporter un accord approprié de la direction, un historique vérifiable de tous les changements et une révision annuelle de l'autorisation d'accès et d'une réhabilitation des accès excessifs.
Le Fournisseur établira, maintiendra et appliquera les principes d'accès de sécurité de la « ségrégation des tâches » et de « double vérification (Dual Control) » et du « moindre privilège » en ce qui concerne les Biens D'EPSA MARKETPLACE et les Données personnelles du Client.

Le Fournisseur enregistrera et conservera les journaux de tous les accès aux Biens EPSA MARKETPLACE, aux
Données personnelles du Client et au système informatique du Client par son personnel, ses agents ou sous-traitants et ces journaux seront communiqués au Client.

Si le Fournisseur fournit des Services au Client à partir de ses locaux, il respectera le Plan de Prévention communiqué par le Client dans la mesure où il serait applicable aux services et aux technologies informatiques livrés dans le cadre de l'exécution des Services ou nécessaires à la réalisation des Services.

Sécurité physique et environnementale

Dans le cas de Services exécutés hors site Client connectés au système informatique EPSA MARKETPLACE, le
Fournisseur indiquera les emplacements géographiques dans lesquels il exploite les Biens D'EPSA MARKETPLACE et
/ou traite les Données personnelles du Client. Notamment, le Fournisseur fournira l'adresse de :

a. son centre de données primaire et/ou de l'installation informatique et,

b. de son site de sauvegarde et/ou de reprise après sinistre.

Sécurité des opérations

Le Fournisseur s'engage à employer des logiciels pris en charge supportés commercialement (par
exemple, logiciel sous maintenance active, y compris système d'exploitation, logiciel libre ou logiciel d'application et/ou similaire) sur tous systèmes qui traitent, stockent ou supportent techniquement les Services /la fabrication des Produits.
Le Fournisseur notifiera le Client à l'avance un (1) an de toute fin de support commercial de tout composant.
Le Fournisseur notifiera le Client un (1) an avant toute fin de support commercial de tout composant.

Le Fournisseur expliquera et détaillera sa plate-forme multi-clients.

Acquisition, développement et maintenance des systèmes

Le Fournisseur utilisera systématiquement des outils de détection des programmes malveillants avant toute livraison de Livrable et fournira au Client un rapport sur la détection de ces programmes malveillants.

Les règles pour le développement des logiciels incluront au minimum:

a. pas d'utilisation d'identifiants codés en dur ;

b. séparation des rôles d'administrateurs et d'utilisateur ;

c. suppression systématique de tous les comptes par défaut utilisés dans le processus de développement et modification du mot de passe par défaut avant la livraison au Client.

Le Fournisseur apportera des preuves sur les points suivants concernant la conception des Produits/ réalisation des Services :

a. les cyber-risques auxquels sont confrontés exposés les Produits et Services seront identifiés et entraîneront la création de contrôles de cybersécurité appropriés à mettre en place ;

b. les sources de données fiables et non fiables seront identifiées (par exemple, les sources de données internes à l'organisation du Client peuvent être considérées comme fiables tandis que d'autres sources de données peuvent être considérées comme non fiables).

Le Fournisseur s'engage à réaliser (au moins tous les ans) une évaluation de vulnérabilité de ses systèmes accédant à ou contenant des Biens D'EPSA MARKETPLACE et/ou des Données personnelles du Client et atténuera les risques ou remédiera aux défauts critiques dans un délai approprié eu égard à l'importance du défaut et la charge de travail nécessaire à la remédiation. Le Fournisseur s'engage à fournir au Client les rapports précisant la date de l'évaluation, l'identité des personnes ayant réalisé l'évaluation et une indication du risque relatif aux vulnérabilités identifiées ainsi que le délai nécessaire pour y remédier. L'évaluation de la menace de vulnérabilité sera réalisée en utilisant des outils et/ou services correspondant aux standards du secteur.

Le Fournisseur mettra en place un processus de contrôle des modifications techniques pour les produits logiciels et matériels.

Gestion des Incidents de Sécurité

Le Fournisseur mettra en place un processus de gestion approfondi et agréé des Incidents de Sécurité pour les réseaux et les systèmes qu'il exploite, comprenant l'identification, la réponse, le confinement, la récupération, la signalisation, la protection des preuves et l'examen des Incidents de Sécurité.

Le Fournisseur s'engage à informer le Client sans délai en cas d'événement, au plus tard vingt-quatre (24) heures après avoir eu connaissance d'un Incident de Sécurité, à l'adresse suivante : Contact@epsa-marketplace.com. La notification devra inclure, à minima :

a. une déclaration ou une description du problème ;

b. le délai de remédiation attendu (si connu) ;

c. le nom et le numéro de téléphone du représentant du Fournisseur que le Client peut contacter pour obtenir des informations complémentaires.

Les preuves liées à un Incident de Sécurité seront recueillies, conservées et présentées par le Fournisseur afin de respecter les règles de preuve applicables devant les juridictions compétentes.

Gestion de la continuité des opérations

Le Fournisseur aura déployé les moyens pour assurer la continuité commerciale et la reprise en cas de sinistre, y compris la résilience des Services/Produits livrés au Client.

Le Fournisseur notifiera le Client en cas de sinistre.

Conformité

Le Fournisseur reconnaît que le Client ou un auditeur indépendant désigné par le Client peut, à ses propres frais, effectuer un audit du respect des engagements de sécurité du Fournisseur sur ses systèmes, processus et procédures et de sa chaîne logistique, ayant une incidence sur les Services/Produits ou les systèmes du Client. Ceci comporte, notamment, la vérification de l'accord et du contrôle d'accès, le contrôle du flux d'information et des journaux d'audit. Le Fournisseur fournira toute la documentation et les justificatifs nécessaires.
En raison de la nature confidentielle et exclusive des opérations du Fournisseur, et afin de protéger l'intégrité et la sécurité de ces opérations et la nature partagée des systèmes qui peuvent être utilisés pour fournir les Services/Produits:

- les parties conviendront à l'avance de la portée des audits ;
- un préavis écrit d'au moins trente (30) jours avant la date prévue de démarrage de l'audit sera donné par le Client et l'audit se produira au maximum une fois par période de douze (12) mois, à moins de circonstances telles que qu'une présomption raisonnable du Client d' Incident de Sécurité; dans ce cas, un audit pourra être réalisé à une date fixée d'un commun accord entre les parties ;
- si l'audit est réalisé par un tiers, ce dernier sera un auditeur expert e, sécurité et agréé par les parties, étant entendu que le Fournisseur ne pourra refuser le tiers auditeur sans motif légitime ;

- l'audit sera conduit conformément aux exigences et contraintes en matière de confidentialité et de non divulgation des parties; et
- l'audit ne saurait perturber de manière non raisonnable l'activité normale du Fournisseur ou ses opérations informatiques.

Nonobstant les dispositions, ci-dessus, le Client conserve le pouvoir discrétionnaire d'engager une inspection de sécurité au titre de la présente section, et il pourra initier l'inspection avant la réalisation des Services/livraison des Produits puis, (i) en cas de tout modification dans la réalisation des Services/livraison des Produits qui pourrait en affecter la sécurité, (ii) à la suite de tout Incident de Sécurité affectant les Services/Produits ou les Biens D'EPSA MARKETPLACE ou les données personnelles du Client, et (iii) en cas de demande du Client ou de demande émanant d'un organisme gouvernemental. Le Fournisseur apportera au Client l'assistance raisonnable éventuellement nécessaire pour permettre au Client de respecter les lois applicables en matière de sécurité.

Le Fournisseur conservera et protégera tout preuve du respect des obligations légales ou contractuelles et seront mises à la disposition du Client si besoin