Plan de Sécurité de l'Information

Revenue Management System (RMS) (SaaS)

Le présent Plan de Sécurité de l'Information (« PSI ») est intégré au Bon de Commande liant Infor au Client désigné dans le présent PSI et détaille les mesures de sécurité actuellement mises en œuvre pour protéger le matériel informatique, l'équipement et la configuration logicielle des systèmes (i) sur lesquels Infor s'appuie pour fournir l'utilisation du Logiciel sous Abonnement (listé dans le Bon de Commande) et des Services d'Abonnement associés (ii) dans lesquels des Données Clients ont été fournies, entrées ou chargées à des fins d'utilisation par ou avec le Logiciel sous Abonnement par le Client ou ses Utilisateurs Autorisés (i et ii ci-après collectivement dénommés les « Systèmes »). Par souci de clarté, les termes commençant par une majuscule qui sont employés dans le présent PSI mais qui n'y sont pas définis ont le sens qui leur a été donné dans le Contrat SaaS (Software as a Service) conclu entre Infor et le Client (le « Contrat »). Le présent PSI ne s'applique pas aux accords portant sur des services managés réalisés par Infor dans le cadre desquels un logiciel Client est hébergé par Infor en vertu d'un contrat de services professionnels distinct.

Les menaces à la sécurité et les mesures conçues pour s'en prémunir sont en constante évolution. A ce titre, Infor se réserve le droit de modifier le présent PSI à tout moment et sans préavis, pour autant qu'Infor maintienne un niveau de sécurité globale des Systèmes et des Données Client a minima équivalent.

1. Normes Générales de Sécurité

Infor met en œuvre des mesures de sécurité sur le plan administratif, technique et physique visant à empêcher toute destruction, perte, accès non autorisé ou altération des Systèmes et des Données Client qu'Infor traite pour le compte du Client, qui : i) ne sont pas moins rigoureuses que celles mises en œuvre par Infor pour la protection de ses propres informations de nature similaire ; ii) ne sont pas moins rigoureuses que les pratiques généralement admises dans le secteur de l'informatique ; et iii) sont exigées par les lois applicables.

1.1. Responsables de la sécurité

Infor a nommé un ou plusieurs responsables de la sécurité en charge de la coordination et du suivi des mesures de sécurité exposées dans le présent PSI.

1.2. Contrôles d'accès

Infor met en place des dispositifs de contrôle d'accès aux Données Client, incluant notamment les mesures suivantes :

i. Infor attribue un identifiant unique à chaque personne bénéficiant d'un accès informatique aux Données Client.

ii. Infor identifie les membres de son personnel qui auront le pouvoir d'attribuer, de modifier ou d'annuler un accès aux Données Client, et restreint l'accès aux Données Client sur la base du principe de moindre privilège. L'accès aux Données Client n'est autorisé qu'aux membres du personnel ayant « besoin d'en prendre connaitre » aux fins de la réalisation des Services d'Abonnement. Infor tient et met à jour un registre desdits membres de son personnel. De tels accès sont enregistrés et contrôlés.

iii. Infor a donné comme directive aux membres du personnel ayant accès aux Données Client de fermer leur session lorsque les ordinateurs sont laissés sans surveillance.

iv. Infor désactive les comptes de ses employés des applications et magasins de données contenant des Données Client lorsqu'il est mis fin au contrat desdits employés ou s'il est transféré, ou lorsqu'ils n'ont plus besoin d'accéder aux Données Client. Infor examine régulièrement la liste des personnes et des services ayant accès aux Données Client et supprime les comptes ne nécessitant plus un tel accès. Infor procède à cet examen au moins deux fois par an.

v. Infor n'utilise, pour aucun des Systèmes, les mots de passe et autres paramètres de sécurité définis par défaut par le fabricant. La société rend obligatoire et systématique, sur tous les Systèmes Infor, l'utilisation de « mots de passe forts », conformément aux meilleures pratiques généralement admises dans le secteur de l'informatique. Infor exige que l'intégralité des mots de passe et identifiants d'accès demeurent

confidentiels et en interdit le partage aux autres membres du personnel. Infor désactive les mots de passe dont elle sait qu'ils ont été compromis ou divulgués.

vi. Infor maintient un « dispositif de blocage de compte » qui désactive les comptes ayant accès aux Données Client lorsqu'un nombre déterminé de tentatives infructueuses de saisie de mot de passe est dépassé.

vii. L'accès à distance aux Systèmes contenant des Données Client par Infor CloudOps nécessite une authentification à deux facteurs (i.e. au moins deux facteurs différents sont nécessaires à l'identification des utilisateurs).

1.3. Détection et Prévention des Intrusions

Infor utilise un système de détection d'instruction / un système de prévention d'intrusion (IDS/IPS) pour surveiller ses Systèmes et procédures et repérer les failles et violation de la sécurité et toutes activités suspectes. Celles-ci comprennent les activités suspectes extérieures (comprenant notamment les sondes et les scans non autorisés ou les tentatives d'intrusion) et les activités suspectes internes (comprenant notamment les accès aux Systèmes par des administrateurs non autorisés, les modifications non autorisées des Systèmes, l'utilisation impropre ou le vol des Systèmes, ou l'utilisation non autorisée des Données Client). Infor examine régulièrement les journaux d'accès en vue de détecter tout comportement malveillant ou accès non autorisé.

1.4. Pare-feu

Infor maintient un pare-feu réseau conçu pour la protection des Données Client accessibles depuis Internet.

1.5. Mise à jour

Infor maintient les Systèmes à jour en installant les mises à niveau, les mises à jour, les correctifs et les nouvelles versions.

1.6. Chiffrement des données

Les Données Client transitant par des réseaux publics sont chiffrées au minimum avec TLS 1.2 ou toute technologie plus récente lui succédant.

1.7. Gestion des Identités

Infor utilise un modèle de sécurité partagé. Infor a la possibilité de fédérer les applications dans les Systèmes jusqu'au fournisseur de solution de gestion de l'identification du Client.

1.8. Logiciels malveillants

Infor utilise des logiciels contre les logiciels malveillants et antivirus répondant aux standards généralement reconnus et mis en place dans le secteur de l'informatique et, dans la mesure du possible, a recours à des dispositifs de protection en temps réel afin de s'efforcer de fournir un Logiciel sous Abonnement et des Services d'Abonnement exempts de « bombes à retardement », de « vers informatiques », de « virus », de « chevaux de Troie », de « codes de protection », de « clés de destruction de données » ou d'autres programmes conçus pour accéder aux Données Client, pour modifier, supprimer, endommager ou désactiver lesdites Données ou pour en empêcher ou en limiter l'accès par le Client (« Code Malveillant »).

1.9. Sécurité physique

Les installations accueillant les Systèmes :

i. sont structurellement conçues pour supporter des conditions météorologiques défavorables et d'autres événements naturels prévisibles ;

ii. disposent de dispositifs de protection environnementale appropriés en vue de protéger les Systèmes contre la fumée, la chaleur, l'eau, l'humidité ou les fluctuations dans l'alimentation électrique ;

iii. disposent de systèmes d'alimentation électrique de secours sur site ;

iv. assurent des contrôles appropriés en vue de ne garantir l'accès aux installations qu'aux seuls membres du personnel dûment habilités.

2. Audit

2.1. Droits d'audit

Dans le cadre du contrôle de ses fournisseurs, le Client et, le cas échéant, son autorité publique de régulation peuvent demander, dans la limite d'une fois par an et sous la forme d'un audit documentaire réalisé par voie postale (c'est-à-dire par le biais d'un questionnaire reposant sur la norme ISO 27001), la communication des documents procéduraux d'Infor concernant son programme, ses procédures et ses contrôles en matière de sécurité de l'information. Infor accepte, sous réserve que ces documents procéduraux soient immédiatement disponibles, de fournir les documents que le Client pourrait raisonnablement demander, à condition que lesdits documents ne constituent pas a) une menace pour la confidentialité, l'intégrité ou la disponibilité des données ou des services d'autres clients d'Infor ou b) une violation de la confidentialité, de l'intégrité et de la disponibilité des données ou des services de tiers fournissant des Services d'Abonnement aux clients d'Infor pour le compte d'Infor. Les documents procéduraux fournis par Infor ne contiennent aucune preuve (incluant par exemple, notamment une attestation de formation, un justificatif de test ou des résultats d'évaluations des risques). Infor s'engage à répondre au questionnaire sous 30 jours, étant précisé que si ce délai ne peut être respecté, Infor se concertera avec le Client pour trouver un accord sur le délai de réponse. L'ensemble de ces documents procéduraux et le questionnaire constituent des Informations Confidentielles d'Infor. Infor n'examinera pas les conclusions du Client résultant de cet audit .

2.2. Audit de tiers

Dans la limite d'une fois par an pendant la Durée de l'Abonnement, Infor fera procéder, à ses propres frais, par un auditeur indépendant dûment qualifié, à une évaluation de l'efficacité de la conception et du fonctionnement des objectifs de contrôle définis par Infor et des activités associées en lien avec les Services d'Abonnement. Infor fera procéder par l'auditeur à l'élaboration d'un rapport conforme aux standards établi par le « Statement on Standards for Attestation Engagements No. 18 » (Déclaration sur les standards relatifs aux missions d'attestation n° 18) de l'American Institute of Certified Public Accountants (Institut américain des comptables publics certifiés) ou tout standard équivalent, ledit rapport pouvant comprendre l'ISAE 3402 (le « Rapport d'Audit »). Le Rapport d'Audit constitue une Information Confidentielle d'Infor, auquel le Client peut accéder par l'intermédiaire du portail de maintenance d'Infor. Le Client est en droit de communiquer une copie du Rapport d'Audit à ses auditeurs et autorité(s) publique(s) de régulation, à condition que ceux-ci soient informés du caractère confidentiel de ce Rapport d'Audit et de la nécessité de le protéger en conséquence.

En outre, dans la limite d'une fois par an pendant la Durée de l'Abonnement, Infor fera procéder, à ses propres frais, par un auditeur indépendant dûment qualifié, à une analyse de la sécurité de l'information en relation avec les Services d'Abonnement de certains Logiciels sous Abonnement hébergés dans un environnement partagé et listés sur trust.infor.com, en conformité avec la norme ISO 27001. Infor fera procéder par l'auditeur à l'élaboration d' un rapport conforme à la norme 27001 de l'Organisation internationale de normalisation (ISO). Le rapport d'audit ne sera pas mis à disposition du Client ; néanmoins, ce dernier pourra obtenir à tout moment une copie du certificat correspondant à partir du site internet relatif à la sécurité cloud d'Infor (trust.infor.com). Le certificat fera mention des Logiciels sous Abonnement couverts par le rapport. Dans le cadre de la certification ISO 27001, Infor gère un manuel de Système de gestion de la sécurité de l'information pour chaque Logiciel sous Abonnement couvert par le certificat, de même que pour les Services d'Abonnement associés, ce qui contribue à assurer la protection, la confidentialité, l'intégrité et la disponibilité des actifs d'Infor utilisés aux fins de fournir les Services d'Abonnement.

3. Gestion des Modifications

Infor suit une procédure de contrôle des modifications régissant l'identification et la mise en œuvre des modifications affectant les actifs utilisés pour la fourniture des Services d'Abonnement d'Infor afin d'empêcher toute modification non souhaitée du code source des applications, des interfaces, des systèmes d'exploitation ou des modifications en arrière-plan des données dans les champs et tableaux existants. Toutes les modifications devant être apportées aux actifs utilisés pour la fourniture des Services d'Abonnement doivent suivre une procédure de contrôle des modifications. Infor documente et maintient un registre détaillé du suivi de cette procédure, incluant notamment un système de tickets, et l'enregistrement des procédures de test pour toute modification, comprenant notamment la date et l'heure des modifications ainsi qu'une description de leur nature.

4. Séparation des Données Client, Non-exploitation

4.1. Séparation

Les Données Client sont conservées de manière séparée des données d'Infor et de celles des autres clients d'Infor à l'aide de moyens techniques appropriés.

4.2. Non-exploitation ; Statistiques Agrégées

Les Données Client sont des Informations Confidentielles du Client, et le Client détient l'ensemble des droits de propriété relatifs à ses Données Client. Infor n'exploite pas commercialement les Données Client, n'y accède que dans la mesure où cela est nécessaire à l'exécution des Services d'Abonnement et afin de remplir ses obligations conformément au Contrat.

Infor peut recueillir des Statistiques Agrégées, qui sont la propriété exclusive d'Infor et ne sont pas considérées comme des Données Client. Les « Statistiques Agrégées » sont des données statistiques et des indications de performance générées par des systèmes de mesure et d'enregistrement qui concernent l'utilisation et l'exploitation par le Client des Logiciels sous Abonnement et des Services d'Abonnement.

5. Gestion des Actifs

Infor dispose d'un processus formel de gestion des actifs comprenant :

i. la tenue d'un inventaire des actifs utilisés pour la fourniture des Services d'Abonnement (« Actifs »), la définition claire de la propriété et du contrôle des Actifs, la capacité d'identifier des Actifs et la gestion de la restitution, de la destruction ou du retrait des Données Client des Actifs concernés ;

ii. des procédures conçues pour protéger les Actifs contre les menaces et les vulnérabilités, internes comme externes, délibérées comme accidentelles.

6. Recherche de vulnérabilités et Test de Pénétration

Infor dispose d'un processus de gestion des vulnérabilités visant à repérer les risques résultant de l'exploitation (accidentelle ou intentionnelle) de failles publiées ou identifiées qui pourraient être à l'origine de dommages ou d'accès non autorisés aux Systèmes (« Vulnérabilités »). Infor traite les Vulnérabilités dans des délais considérés comme globalement acceptables dans le secteur informatique. Infor corrige ou atténue les Vulnérabilités d'une manière proportionnée au risque qu'elles représentent, dans le cadre défini par Infor, qui est conforme aux standards généralement admis dans le secteur de l'informatique.

Une fois par an, Infor fait procéder, à ses propres frais, par un tiers indépendant à des tests de pénétration, incluant des tests opérés de manière manuelle, afin d'évaluer les contrôles de sécurité des Systèmes hébergés dans un environnement partagé, selon des méthodologies généralement reconnues dans le secteur de l'informatique.

Pour certains Logiciels sous Abonnement dont l'hébergement est réalisé au sein d'un environnement partagé, des tests d'évaluation de la sécurité, notamment des analyses du code source et des recherches de Vulnérabilités, sont conduites en amont de la mise à disposition des Logiciels sous Abonnement et tout au long de la durée de vie de ces Logiciels sous Abonnement (c.-à-d. dans des environnements de développement et de production) pour repérer les Vulnérabilités potentielles afin d'y remédier ou de les atténuer. De manière annuelle, des tests de pénétrations sont réalisés sur certains des Systèmes hébergés dans des environnements partagés pour identifier les Vulnérabilités afin d'y remédier ou de les atténuer.

7. Réponse aux Incidents Relatifs à la Sécurité de l'Information

Si Infor a connaissance, d'une utilisation ou d'une divulgation avérée ou présumée, non autorisée par ce PSI, des Données Clients (« Incident affectant la Sécurité de l'Information ») la société s'engage à : (i) aviser le Client dans les meilleurs délais (et, en tout état de cause, dans les 48 heures après avoir pris connaissance de l'Incident affectant la Sécurité de l'Information) de la survenance d'un tel événement ; (ii) examiner et procéder à une analyse raisonnable des causes de l'Incident affectant la Sécurité de l'Information ; (iii) informer régulièrement le Client des progrès de l'analyse en cours ; (iv) élaborer et mettre en œuvre les mesures appropriées pour remédier à la cause de l'Incident affectant la Sécurité de l'Information, dans la mesure où une telle remédiation est sous le contrôle raisonnable d'Infor ; et (v) fournir au Client une coopération raisonnable dans le cadre de son analyse ou afin que ce dernier puisse se conformer à son obligation de notification ou à toute autre exigence réglementaire applicable à cet Incident affectant la Sécurité de l'Information. À la demande du Client, et à ses frais, en cas d'Incident affectant la Sécurité de l'Information, Infor communiquera (dans la mesure où la loi le permet et sous réserve de la mise en œuvre de mesures de protection appropriées en matière de confidentialité) des copies des registres d'activités

relatifs aux Systèmes (uniquement en lien avec l'Incident affectant la Sécurité de l'Information qui concerne le Client) au Client uniquement aux fins d'utilisation dans le cadre d'une procédure légale ou réglementaire ou d'une enquête gouvernementale.

8. Enregistrement et Contrôle

Infor surveille les ressources utilisées pour la fourniture des Services d'Abonnement par l'intermédiaire de plusieurs outils spécialement conçus pour gérer les journaux et les alertes. Les registres sont protégés physiquement et virtuellement afin d'éviter toute tentative de falsification. Les informations sensibles et les mots de passe ne sont, en aucun cas, enregistrés. Outre la saisie des informations relatives aux Services d'Abonnement, les outils de surveillance permettent aux administrateurs de suivre l'activité des utilisateurs lorsqu'ils entrent et sortent du système.

9. Sécurité en matière de Ressources Humaines

Les membres du personnel d'Infor qui fournissent les Services d'Abonnement sont soumis à des obligations de confidentialité, connaissent les menaces et les préoccupations en matière de sécurité de l'information, reçoivent une formation en matière de sécurité au moins une fois par an et sont en mesure de soutenir la mise en œuvre des politiques organisationnelles en matière de sécurité de l'information de manière générale mais également dans le cadre de leurs propres fonctions.

10. Contrôles des points de terminaison (Ordinateurs Portables, Postes de Travail et Appareils Mobiles d'Infor)

Infor met en œuvre les mesures de sécurité généralement reconnues et appliquées au sein du secteur de l'informatique pour la protection des points de terminaison, notamment l'automatisation de la gestion des correctifs pour les applications et les systèmes d'exploitation et la protection antivirus.

11. Restitution et Effacement des Données

11.1. Restitution En cas de résiliation ou d'expiration du Bon de Commande relatif aux Services d'Abonnement, Lors de la résiliation ou de l'expiration des Services d'abonnement, toutes les données de tout système de rendement seront supprimées et ne seront pas transférées au Client.. Dans le cas où le Client exigerait la restitution des Données Client dans un autre format ou demanderait d'autres services d'assistance liés à la résiliation ou à l'expiration du Bon de Commande, Infor et le Client devront convenir par contrat écrit séparé du périmètre de ces services d'assistance et des prix et frais dus au titre de ceux-ci.

11.2. Destruction

Infor efface définitivement toutes les occurrences (accessibles en ligne ou sur le réseau) des Données Client dans les 30 jours suivant la résiliation ou l'expiration du Bon de Commande relatif aux Services d'Abonnement. Infor utilisera les processus généralement reconnus et appliqués au sein du secteur de l'informatique pour éliminer le matériel et les composants physiques contenant les Données Client. Tout l'archivage est effacé électroniquement (mis à zéro) avant d'être déployé au sein de ou retiré de l'environnement de production d'Infor.

12. Sous-traitants

Les sous-traitants qui fournissent des biens et des services à Infor en lien avec les Services d'Abonnement le font à des conditions substantiellement similaires à celles énoncées dans le présent PSI. Avant de recruter un tel sous-traitant tiers pour réaliser l'un des Services d'Abonnement prévus, Infor examine ce sous-traitant avec une diligence raisonnable afin de s'assurer que ce tiers est en mesure de respecter les obligations de confidentialité et de sécurité stipulées au présent PSI. Infor est responsable des actions de ses sous-traitants qui agissent pour son compte dans le cadre de la fourniture des Services d'Abonnement.