Plan de Sécurité de l'Information

Anael (France)

Périmètre : Le présent Plan de Sécurité de l'Information (« PSI ») est intégré aux contrats conclus entre le Client et Infor (ensemble les « Contrats »). En cas de conflit ou incohérence entre les termes du présent PSI et les termes des Contrats, les termes du présent PSI prévalent sur ceux des Contrats. Le présent PSI détaille les mesures de sécurité actuellement mises en œuvre par Infor de manière générale à l'égard de l'ensemble des Clients pour protéger :

(i) le matériel informatique, l'équipement et la configuration logicielle des systèmes sur lesquels Infor fournit :

- les Services Cloud (les Services Cloud incluent la Maintenance),
- les Services Professionnels, et
- la Maintenance relative au Logiciel sur Site

(lesquels matériel informatique, équipement, et configuration logicielle des systèmes sont collectivement définis dans le présent PSI comme « Systèmes », et les Services Cloud, Services Professionnels et la Maintenance du Logiciel sur Site sont collectivement désignés dans le présent PSI comme les « Services ») ; ainsi que

(ii) les données Clients fournies à Infor, soit :

- en tant que Données Clients, ou
- aux fins de réalisation des Services Professionnels et/ou de la Maintenance dans l'environnement d'Infor (lesquelles données sont collectivement désignées dans le présent PSI comme « Données »).

Définitions : Les termes commençant par une majuscule dans le présent PSI mais qui n'y sont pas définis ont le sens qui leur a été donné dans le Contrat de Licence de Logiciel conclu entre Infor et le Client (le « Contrat »).

Exclusions : Le présent PSI ne s'applique pas: (i) aux accords portant sur des Services Professionnels réalisés par Infor dans le cadre desquels un Logiciel sur Site du Client est hébergé par Infor en vertu d'un contrat de Services Professionnels distinct, ou (ii) quand Infor réalise des services sur le site du Client et/ou reçoit un accès aux systèmes du Client. Dans de tels cas, Infor devra se soumettre aux conditions administratives, techniques et physiques du Client, telles qu'elles auront été définies de manière conjointe dans un ordre de Services, et dans le cadre d'un tel accès aux systèmes du Client, le Client aura la charge de fournir au personnel d'Infor les autorisations et mots de passe utilisateurs afin d'accéder à ses systèmes, ainsi que de retirer de telles autorisations et mettre fin à ces accès, de la manière dont le Client le juge approprié.

Mise à jour : 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 a minima équivalent.

1. Normes Générales de Sécurité

Infor maintient 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, 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. Infor décline toute responsabilité à l'égard des systèmes d'exploitation tiers, ainsi que des produits et services tiers interopérant avec les Systèmes et que le Client (a) développe ou a développé pour son propre compte, ou (b) acquiert sous licence en vertu des conditions de licence applicables de ces tiers.

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, incluant, sans s'y limiter, notamment les mesures suivantes :

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

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

iii. Infor a donné comme directive aux membres du personnel ayant accès aux Données 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 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. Infor examine régulièrement la liste des personnes et des services ayant accès aux Données 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. Infor 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 lorsqu'un nombre déterminé de tentatives infructueuses de saisie de mot de passe est dépassé.

vii. L'accès aux applications Anael ne se fait pas via Internet mais via un lien dédié spécifique au VPN.

1.3. **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.

1.4. **Chiffrement des données**

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

1.5. **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 des Services Cloud, ou des Logiciels sur Site, 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 (i) en rapport avec les Services Cloud modifier, supprimer, endommager ou désactiver les Données ou pour en empêcher ou en limiter l'accès par le Client ou (ii) en rapport avec les Logiciels sur Site modifier, supprimer, endommager ou désactiver les Données du Client au sein du Logiciel sur Site.

1.6. **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. **Séparation des Données, Non-exploitation**

2.1. **Séparation**

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

2.2. **Non-exploitation ; Statistiques Agrégées**

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

Infor collecte des données statistiques et des informations de performance générées par des systèmes d'instrumentation et de journalisation, relatives à l'utilisation et au fonctionnement des Services par le Client (ci-après les "Statistiques Agrégées"). Les Statistiques Agrégées sont la propriété exclusive d'Infor et ne sont pas considérées comme des Données.

3. **Gestion des Actifs**

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

i. d'un inventaire des actifs utilisés pour la fourniture des Services (« Actifs ») destinés à identifier et définir clairement la propriété et le contrôle des Actifs ;

ii. des procédures conçues pour gérer la restitution, la destruction ou le retrait des Données des Actifs concernés ; et

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

4. **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.

Pour les Services Cloud hébergés dans 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 Services Cloud et tout au long de la durée de vie de ces Services Cloud (c.-à-d. dans des environnements de développement et de production) pour repérer les Vulnérabilités potentielles afin d'y remédier ou de les atténuer.

5. **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 le Contrat, des Données (« Incident affectant la Sécurité de l'Information ») la société s'engage à : (i) aviser un Client concerné 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.

6. **Enregistrement et Contrôle**

Infor surveille les ressources utilisées pour la fourniture des Services par l'intermédiaire de plusieurs outils spécialement conçus pour gérer les journaux et les alertes. Les informations sensibles et les mots de passe ne sont, en aucun cas, enregistrés. Outre la saisie des informations relatives aux services, les outils de surveillance permettent aux administrateurs de suivre l'activité des utilisateurs lorsqu'ils entrent et sortent du Système.

7. **Sécurité en matière de Ressources Humaines et Formation**

Les membres du personnel d'Infor qui fournissent les Services 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.

8. **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.

9. Restitution et Effacement des Données

9.1. Restitution

Avant la résiliation, le Client a accès aux Données Client par le biais d'interfaces applicatives et en cas de résiliation ou d'expiration des Services Cloud, Infor mettra à disposition du Client sans délai (dans un délai de 3 à 5 jours ouvrables à compter de la réception de la demande écrite du Client par soumission d'un ticket de Maintenance standard, ladite demande devant être formulée dans un délai de 30 jours suivant la résiliation, (10 jours dans le cas d'un single-tenant)) toutes les Données Client via un export dans le format natif de la base de données par le biais du service de transfert de fichiers sécurisé d'Infor. 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.

En outre, pour plus de clarté, la restitution ou destruction des Données Personnelles se fera en accord avec les termes de l'Avenant relatif à la Protection des Données.

Les données liées aux systèmes de rendement (par exemple, Infor Document Management, Infor EzRMS ou Infor Hospitality Price Optimizer) sont supprimées lors de la résiliation et ne sont pas transférées au Client.

9.2. Destruction

Sauf en ce qui concerne l'Assistance à la Transition demandée par le Client, 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 des Services Cloud en accord avec NIST 800-88.

Les Données fournies à Infor aux fins de fourniture de la Maintenance (c'est-à-dire par le biais d'un ticket de Maintenance enregistré sur le portail de Maintenance) sont supprimées cinq ans après la date de clôture de l'incident. Le nom individuel et les informations de contact du Client (par ex. adresse email, nom et numéro de téléphone) utilisés pour gérer le cycle de vie du ticket de Maintenance est désactivé et anonymisé à la résiliation de la Maintenance.

10. Sous-traitants

Les sous-traitants qui fournissent des biens et des services à Infor en lien avec les Services 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 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.