Plan de Sécurité de l'Information Nexus*

** Produits Nexus Applicables: Nexus AppXpress (SaaS), Nexus Live Visibility (SaaS), Nexus Factory Management (SaaS), Nexus Inventory Management (SaaS), Nexus Supply Chain Finance (SaaS), Nexus Supply Collaboration (SaaS), Nexus Transportation Management (SaaS), Nexus Supply Chain Visibility (SaaS), Nexus Procure to Pay (SaaS), Nexus Supply Chain Intelligence (SaaS).*

MISE A JOUR NOVEMBRE 2024

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 pour protéger :

i. le matériel informatique, l'équipement et la configuration logicielle des systèmes sur lesquels Infor s'appuie pour fournir :
   - les Services Cloud (par soucis de clarté, les Services Cloud incluent la Maintenance)
   - Les Services Professionnels ;
     (le matériel informatique, l'équipement et la configuration logicielle des systèmes sont ci-après collectivement dénommés les « Systèmes » et les Services Cloud, les Services Professionnels et la Maintenance relative aux Logiciels sur Site sont ci-après collectivement dénommés les « Services ») ; et

ii. Les données client fournies à Infor, soit :
   - en tant que Données Client, ou
   - communiquées à Infor aux fins de la réalisation des Services Professionnels et/ou de Maintenance depuis l'environnement d'Infor
     (de telles données sont collectivement dénommées les « Données »)

Définition : 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 de Licence de Logiciel conclu entre Infor et le Client (le « Contrat »).

Exclusions : Le présent PSI ne s'applique pas lorsqu'Infor fournit des services dans les locaux du Client et/ou a accès aux systèmes du Client. Dans de tels cas, Infor doit se conformer aux dispositions administratives, techniques et physiques du Client convenues d'un commun accord dans un ordre de services, et dans le cadre d'un tel accès aux systèmes du Client, le Client est responsable de la fourniture au personnel d'Infor des autorisations et mots de passe utilisateurs nécessaires pour accéder à ses systèmes et de la révocation de ces autorisations et accès, dès lors que le Client le juge approprié.

Mises 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.

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.

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. Les applications utilisent des délais d'attente pour désactiver les sessions après une période donnée.

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 à distance aux Systèmes contenant des Données 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). Infor examine régulièrement les journaux d'accès en vue de détecter tout comportement malveillant ou accès non autorisé.

1.4. Pare-feu

Infor a mis en place et maintient des technologies de pare-feu réseau conçues pour la protection des Données accessibles par 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

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

ii. Tant que les Données sont stockées dans les Systèmes, mais elles sont tout de même chiffrées au minimum avec AES 256 bits ou toute technologie plus récente lui succédant.

1.7. Gestion des Identités

Infor s'appuie sur un modèle de sécurité partagé pour répartir les responsabilités en matière de gestion des identités. Infor a la possibilité de fédérer les applications dans les Systèmes jusqu'au fournisseur de solution de gestion de l'identification du Client à des fins d'authentification.

1.8. Signature Unique (Single Sign On)

Infor Nexus supporte le système central de Single Sign On [SSO] en utilisant les systèmes tiers d'un client en tant que fournisseur d'identité (IDP) et Infor Nexus en tant que fournisseur de services. Infor Nexus prend en charge tous les systèmes de fournisseurs d'identité utilisant les normes SAML (Security Assertion Markup Language) 2.0. La Signature Unique du client est supposée avoir une authentification à deux facteurs.

1.9. Directives de Sécurité

Les recommandations d'authentification d'Infor Nexus sont préparées en accord avec les directives du National Institute of Standards and Technology (NIST) des Etats-Unis et les meilleures pratiques généralement acceptées dans l'industrie.

1.10. Système de sécurité à deux facteurs

Infor Nexus recommande toujours l'utilisation d'une authentification à deux facteurs. L'utilisateur peut utiliser l'application mobile Infor Nexus pour le 2e facteur d'authentification. Cependant, les utilisateurs du produit Procure to Pay sont tenus d'utiliser l'authentification à deux facteurs.

1.11. Gestion des mots de passe

Dans les cas où la Signature Unique n'est pas disponible, les clients d'Infor Nexus sont responsables de la configuration d'une politique de mot de passe conforme aux normes de sécurité de leur entreprise. Tous les comptes du Client adhéreront à cette politique de mot de passe.

Les paramètres de mot de passe par défaut sont les suivants

- Tous les mots de passe sont comparés à des mots de passe réels précédemment exposés lors de violations de données. Les mots de passe figurant sur cette liste ne sont pas autorisés.
- Tous les mots de passe doivent comporter au moins 8 caractères.
- Les espaces sont autorisés dans les mots de passe, et l'utilisation d'une phrase facile à retenir est encouragée.
- Aucun des éléments suivants n'est autorisé, à moins que le mot de passe ne contienne au moins 8 caractères supplémentaires (ou le minimum configuré, supérieur à 8) :
    - Le nom ou le prénom de l'utilisateur
    - Le login de l'utilisateur
    - Tout mot du nom de l'organisation de l'utilisateur supérieur à trois caractères
    - Le numéro de téléphone et le numéro de fax de l'utilisateur ou de l'organisation
    - L'adresse électronique de l'utilisateur

1.12. Mesures Intégrées

Pour empêcher le cassage des mots de passe par force brute, un algorithme d'étranglement empêchera les tentatives de deviner le mot de passe. Les clients peuvent configurer leur politique en matière de mots de passe :

- Longueur minimale du mot de passe (supérieure à 8)
- Utilisation obligatoire de lettres majuscules et minuscules dans le mot de passe
- Utilisation obligatoire de chiffres dans le mot de passe
- Utilisation obligatoire de symboles dans le mot de passe
- Utilisation obligatoire de chiffres ou de symboles dans le mot de passe
- Expiration du mot de passe après un certain nombre de jours
- Comptes d'utilisateurs verrouillés après un certain nombre de tentatives de saisie du mot de passe

Le mot de passe minimum est de 8 par défaut et ne peut être abaissé. Le reste de ces paramètres, en accord avec les meilleures pratiques modernes, ne sont pas définis par défaut, mais peuvent être configurés pour les organisations du Client par Infor Nexus dans le cadre de l'implémentation.

1.13. 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 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 modifier, supprimer, endommager ou désactiver les Données Client ou pour en empêcher ou en limiter l'accès par le Client.

1.14. 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 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 convenu d'un commun accord pour l'exécution des travaux. 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 Cloud (à l'exception de la Maintenance). Infor fera procéder par l'auditeur à l'élaboration d'un rapport SOC II Type 2 et, le cas échéant, un rapport SOC I Type 2 pour les Services Cloud (collectivement 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.

3. Gestion des Modifications pour les Services Cloud

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 Cloud 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 Cloud 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, Non-exploitation

4.1. 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.

4.2. 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.

En ce qui concerne les Données, 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 Services.

5. 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 ») conçu pour 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 ;

iii. 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 sur les Services Cloud hébergés dans un environnement partagé, incluant des tests opérés de manière manuelle, afin d'évaluer les contrôles de sécurité des Systèmes, selon des méthodologies généralement reconnues 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. De manière annuelle, des tests de pénétrations sont réalisés sur les Services Cloud 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 le Contrat, des Données (« Incident affectant la Sécurité de l'Information ») Infor s'engage à : (i) aviser le 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.

8. Enregistrement et Contrôle

Infor surveille les ressources utilisées pour la fourniture des Services Cloud 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 Cloud, 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 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.

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 des Données

Le Client a accès à ses données pendant toute la durée de son abonnement, sous réserve des temps d'arrêt prévus, de la maintenance d'urgence et des autres directives relatives à la disponibilité du niveau de service. 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. Nonobstant ce qui précède, les Données partagées doivent rester sur la Plateforme Infor Nexus car elles ne sont pas la propriété du Client, elles sont partagées. Les Données Partagées sont toutes les données qui sont visibles à la fois par le Client/Membre et par un ou plusieurs autres membres autorisés sur la Plateforme Infor Nexus, tels que les fournisseurs et les prestataires de services. Les données sont stockées au niveau de la transaction et non au niveau du client.

Les Données communiquées à Infor à des fins d'exécution de la Maintenance (c'est-à-dire via un ticket de Maintenance sur le portail de Maintenance) sont purgées cinq ans à compter de la date de clôture du ticket incident. Le nom individuel du Client et ses coordonnées (par exemple, l'adresse e-mail, le nom et le numéro de téléphone de l'utilisateur) utilisés pour gérer le cycle de vie des tickets de Maintenance sont désactivés et anonymisés à la fin de la Maintenance.

12. 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.