Information Security Plan
Annexe Règlementaire de l'UE

La présente Annexe décrit les engagements d'Infor concernant les exigences spécifiques en vertu des directives, règlements et lois nationales de mise en œuvre de l'UE applicables en matière de cybersécurité et de gouvernance des données (« **Droit Applicable en matière de Cybersécurité et de Gouvernance des Données** »), et est intégrée, le cas échéant pour le Client (avec applicabilité telle que définie ci-dessous), aux accords du Client conclus avec Infor (collectivement, les « **Contrats** »). En cas de conflit ou d'incohérence entre les termes de la présente Annexe et les autres termes des Contrats, la présente Annexe prévaut.

I. GÉNÉRALITÉS

1. DÉFINITIONS

1.1 Les termes commençant par une majuscule utilisés mais non définis dans la présente Annexe auront les significations fournies dans le Plan de Sécurité de l'Information, situé à l'adresse www.infor.com/security-plan (le « PSI »). Les termes « Processus TIC », « Produit TIC », « Service TIC », « Incidents », « Systèmes Réseaux et Information », « Risque », et « Menace Cybernétique Significative » auront la signification qui leur est donnée dans le Droit Applicable en matière de Cybersécurité et de Gouvernance des Données.

2. CONFORMITÉ ET COOPÉRATION

2.1 Infor se conformera au Droit Applicable en matière de Cybersécurité et de Gouvernance des Données applicables à son entreprise et, sur demande raisonnable, coopérera avec toute autorité gouvernementale compétente et/ou le Client concernant la conformité d'Infor à ses obligations en vertu des Contrats relatives au Droit Applicable en matière de Cybersécurité et de Gouvernance des Données. Infor et le Client s'informent et s'alertent mutuellement de tout changement significatif ou événement, difficulté, risque ou information susceptible d'avoir un effet défavorable sur les Services TIC ou la performance des Contrats (sauf si le partage de telles informations est interdit par la Loi Applicable).

3. DATE D'EFFET

3.1 Les termes de la présente Annexe prennent effet à la date à laquelle le Droit Applicable en matière de Cybersécurité et de Gouvernance des Données devient effectif et exécutoire.

4. MISES À JOUR

4.1 Le Client reconnaît que les mesures de sécurité techniques et organisationnelles décrites dans la présente Annexe sont soumises à des mises à jour requises en vertu du Droit Applicable en matière de Cybersécurité et de Gouvernance des Données et aux progrès techniques et au développement, et qu'Infor peut mettre à jour ou modifier les mesures de temps en temps, à condition que ces mises à jour et modifications ne dégradent pas la sécurité globale des Services fournis au Client.

5. LOI APPLICABLE

5.1 La présente Annexe est régie par et appliquée conformément au choix du droit défini dans les Contrats, sauf si un autre choix de droit est requis par le Droit Applicable en matière de Cybersécurité et de Gouvernance des Données, auquel cas, aux fins de la présente Annexe, le choix du droit ainsi requis prévaudra sur le choix du droit défini dans les Contrats.

6. RESPONSABILITÉ

6.1 Infor et le Client conviennent que la responsabilité totale de chaque partie et de ses Affiliés (tels que définis dans les Contrats) découlant de ou en relation avec la présente Annexe, qu'elle soit basée sur une rupture de contrat, un délit ou autre, est, entre les parties (y compris les Affiliés), soumise aux dispositions applicables sur la limitation de responsabilité dans les Contrats. De plus, Infor ne sera pas responsable de toute violation par le Client du Droit Applicable en matière de Cybersécurité et de Gouvernance des Données ou d'un manquement du Client à se conformer aux exigences de l'autorité compétente.

II. DIRECTIVE NIS 2

1. PÉRIMÈTRE ET DÉFINITIONS

1.1 Les termes et conditions énoncés dans la Section II de la présente Annexe s'appliquent uniquement aux Clients de l'UE qui répondent aux critères et seuils d'entités « importantes » ou « essentielles » qui sont régulées par la Directive NIS 2. Pour éviter toute ambiguïté, la Section I est réputée incorporée à cette Section II.

1.2 « **Directive NIS 2 »** désigne la Directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 relative à des mesures pour un niveau commun élevé de cybersécurité dans l'UE, modifiant le Règlement (UE) No 910/2014 et la Directive (UE) 2018/1972, et abrogeant la Directive (UE) 2016/1148, et toute réglementation de mise en œuvre correspondante.

2. GOUVERNANCE

2.1 Infor dispose d'organes de gestion au sein de son bureau de sécurité qui approuvent, supervisent et sont responsables de la mise en œuvre des mesures de gestion des risques de cybersécurité d'Infor, y compris le PSI.

3. PROGRAMME DE SÉCURITÉ DE L'INFORMATION

3.1 Infor a mis en œuvre et maintiendra le PSI afin qu'il soit conçu pour : (A) assurer la sécurité et la confidentialité des Systèmes Réseaux et d'Information d'Infor ; (B) protéger contre toute menace ou risque anticipé pour la sécurité ou l'intégrité des Systèmes Réseaux et d'Information d'Infor ; et (C) protéger contre tout accès ou usage non autorisé des Systèmes Réseaux et d'Information ; et établit la politique d'Infor pour répondre à tout Incident.

3.2 Le PSI est disponible à : www.infor.com/security-plan.

4. MESURES DE GESTION DES RISQUES DE CYBERSÉCURITÉ

4.1 Infor a mis en œuvre et maintiendra des mesures de gestion des risques de cybersécurité qui :

(A) sont proportionnées aux risques posés aux Systèmes Réseaux et d'Information d'Infor en tenant compte de l'état de l'art et, le cas échéant, des normes européennes et internationales pertinentes, ainsi que du coût de la mise en œuvre ;

(B) sont basées sur une approche « tous risques », qui vise à protéger les Systèmes Réseaux et d'Information d'Infor ainsi que l'environnement physique de ces systèmes contre les Incidents ; et

(C) incluent au moins les éléments suivants : (a) politiques d'analyse des risques et de sécurité des systèmes d'information ; (b) mesures pour identifier tout risque d'Incidents, y compris les procédures de gestion des incidents ; (c) continuité d'activité, telle que la gestion des sauvegardes et la reprise après sinistre, et gestion de crise ; (d) sécurité de la chaîne d'approvisionnement, y compris les aspects de sécurité concernant les relations entre Infor et ses fournisseurs directs ou prestataires de services ; (e) sécurité dans l'acquisition, le développement et la maintenance des Systèmes Réseaux et d'Information , y compris la gestion et la divulgation des vulnérabilités ; (f) politiques et procédures pour évaluer l'efficacité des mesures de gestion des risques de cybersécurité d'Infor ; (g) pratiques de base en matière d'hygiène cybernétique, telles que les principes de confiance zéro, mises à jour logicielles, configuration des appareils, segmentation du réseau, gestion des identités et des accès ou sensibilisation des utilisateurs, formation régulière à la cybersécurité pour le personnel et sensibilisation aux menaces cybernétiques, techniques d'hameçonnage ou d'ingénierie sociale ; (h) politiques et procédures concernant l'utilisation de la cryptographie et du chiffrement ; (i) sécurité des ressources humaines, politiques de contrôle d'accès et gestion des actifs ; et (j) utilisation de l'authentification multi-facteurs ou de solutions d'authentification continue, communications vocales, vidéo et textuelles sécurisées et systèmes de communication d'urgence sécurisés au sein d'Infor.

5. CHAÎNE D'APPROVISIONNEMENT

5.1 Infor déclare et garantit que les mesures de sécurité de la chaîne d'approvisionnement mises en œuvre par Infor tiennent compte des critères suivants : (a) les vulnérabilités spécifiques à chaque fournisseur direct et prestataire de services d'Infor ; (b) la qualité globale des produits et des pratiques de cybersécurité des fournisseurs et prestataires de services d'Infor, y compris leurs procédures de développement sécurisé ; et, le cas échéant, (c) les résultats de toute évaluation coordonnée des risques de sécurité des chaînes d'approvisionnement de Services TIC,

Produits TIC ou Processus TIC critiques spécifiques réalisée par des États Membres de l'UE et toute autorité compétente.

5.2 Infor effectue une diligence raisonnable sur ses prestataires de services tiers pour évaluer leurs mesures de gestion des risques de cybersécurité et conclut des accords avec ces prestataires de services tiers comportant des exigences de cybersécurité et de gouvernance des données substantiellement similaires à celles de la présente Annexe.

5.3 Infor fournira des preuves raisonnables de telles mesures de sécurité de la chaîne d'approvisionnement dans un délai raisonnable après la demande du Client.

6. RÉPONSE AUX INCIDENTS

6.1 Infor surveillera ses Systèmes Réseaux et d'Information pour détecter tout accès non autorisé et mettra en œuvre une politique de réponse aux Incidents spécifiant les actions à entreprendre lorsque Infor détecte ou prend connaissance de tout Incident.

6.2 Si Infor prend connaissance d'un Incident Significatif affectant le Client, Infor devra :

(A) Notifier le Client comme suit :

(1) Promptement et sans retard injustifié (et en tout cas dans les 24 heures après avoir pris connaissance d'un tel Incident Significatif) : (a) notifier le Client de la survenue d'un tel Incident Significatif ; et (b) fournir au Client des informations détaillées sur l'Incident Significatif, y compris les suivantes : (i) si l'Incident Significatif est soupçonné d'être causé par des actes illégaux ou malveillants ou pourrait avoir un impact transfrontalier ; (ii) toute information permettant de déterminer tout impact transfrontalier de l'Incident Significatif ; et (iii) une évaluation initiale de l'Incident Significatif, y compris sa gravité et son impact, ainsi que, le cas échéant, les indicateurs de compromission ;

(2) Promptement et sans retard injustifié, fournir au Client les informations complémentaires suivantes sur l'Incident Significatif : (a) une description détaillée de l'Incident Significatif, y compris sa gravité et son impact ; (b) le type de menace ou la cause première susceptible d'avoir déclenché l'Incident Significatif ; (c) mesures d'atténuation appliquées et en cours ; et (d) le cas échéant, l'impact transfrontalier de l'Incident Significatif.

(B) Enquêter et mener une analyse raisonnable des causes de cet Incident Significatif ;

(C) Fournir des mises à jour périodiques de toute enquête en cours au Client ;

(D) Développer et mettre en œuvre un plan approprié pour atténuer et remédier à la cause de cet Incident Significatif dans la mesure où cette cause est sous le contrôle d'Infor ; et

(E) Coopérer avec l'enquête raisonnable du Client et les efforts du Client pour se conformer à toute notification applicable à cet Incident Significatif, y compris assister à la rédaction de tout rapport concernant l'Incident Significatif aux autorités compétentes.

6.3 Si Infor prend connaissance d'une Menace Cybernétique Significative affectant le Client (y compris les vulnérabilités d'applications Infor publiées qui répondent à la définition de Menace Cybernétique Significative), Infor devra :

(A) Promptement et sans retard injustifié notifier le Client de cette Menace Cybernétique Significative ;

(B) Fournir au Client des informations détaillées sur l'impact de la Menace Cybernétique Significative sur le Client, telles que connues d'Infor ;

(C) Enquêter et mener une analyse raisonnable des causes de cette Menace Cybernétique Significative ;

(D) Développer et mettre en œuvre un plan approprié pour remédier à la cause de cette Menace Cybernétique Significative dans la mesure où cette Menace Cybernétique Significative se matérialise et que la cause est sous le contrôle d'Infor ; et

(E) Se conformer aux demandes raisonnables du Client pour fournir des informations sur la Menace Cybernétique Significative à utiliser par le Client dans ses notifications à des tiers requises concernant la

Menace Cybernétique Significative, si des notifications sont requises en vertu du Droit Applicable en matière de Cybersécurité et de Gouvernance des Données.

7. AUDIT

7.1 Infor détiendra et maintiendra au moins l'une des certifications et attestations suivantes liées à ses Services Cloud (le cas échéant), et Infor, sur demande écrite du Client, fournira au Client une preuve de telles certifications et/ou attestations :

(1) SSAE SOC 2 Type 2 (également connu sous le nom de AICPA TSC 2014 Type 2)
(2) ISO 27001:2022
(3) FedRAMP

Infor s'assurera que ses prestataires de services tiers détiennent ou maintiennent au moins l'une des certifications et attestations ci-dessus liées aux services que ces prestataires de services tiers fournissent à Infor et/ou aux clients d'Infor, ou fournissent des preuves alternatives satisfaisantes de leurs mesures de gestion des risques de cybersécurité relatives au périmètre des services fournis.

7.2 En plus des rapports d'audit décrits à la Section 7.1 ci-dessus, lorsqu'ils sont demandés par le Client et sous réserve des obligations de confidentialité des Contrats, au maximum une fois par an, sauf si le Client agit conformément à une demande d'une autorité gouvernementale compétente (dans ce cas, les limites annuelles ne s'appliquent pas), Infor répondra rapidement par écrit à toutes les demandes raisonnables ou questionnaires du Client (et/ou de ses agents) concernant le contenu du programme de sécurité d'Infor et fournira des preuves raisonnables de sa conformité aux exigences de la présente Annexe, y compris les copies généralement disponibles de données, documents et informations liés aux Services nécessaires pour aider le Client à se conformer à toute demande ou ordonnance contraignante reçue de toute autorité gouvernementale compétente. Infor fournira les informations pertinentes sans retard injustifié (et en tout état de cause dans le délai prévu dans la demande ou l'ordonnance contraignante que le Client a reçue de l'autorité gouvernementale compétente).

7.3 Le Client peut, une fois par an, auditer la conformité d'Infor à ses obligations en vertu de la présente Annexe, y compris auditer les pratiques de sécurité informatique d'Infor et les environnements de contrôle applicables, conformément au processus décrit dans cette Section 7, uniquement si :

(A) Infor n'a pas fourni suffisamment de preuves de sa conformité avec les mesures de gestion des risques de cybersécurité décrites dans la présente Annexe par le biais des rapports et de la documentation mentionnés à la Section 7.2 ci-dessus, ou, le cas échéant, de tout autre rapport d'audit ou autre information qu'Infor met à la disposition générale de ses clients ;

(B) Un Incident Significatif s'est produit ;

(C) Infor a notifié au Client qu'il est soumis à une demande d'accès gouvernementale liée aux Données Client ;

(D) Un audit est formellement demandé par une autorité gouvernementale compétente ayant juridiction sur le Client ; ou

(E) Le Droit Applicable en matière de Cybersécurité et de Gouvernance des Données confère au Client un droit d'audit direct.

7.4 Avant le début d'un audit, le Client et Infor conviendront mutuellement de la portée, du calendrier, de la durée, des exigences en matière de contrôle et de preuves. Le Client peut utiliser une société d'audit tierce accréditée indépendante pour réaliser l'audit en son nom, à condition que le tiers auditeur soit mutuellement accepté par le Client et Infor (ce qui n'inclura pas les auditeurs tiers qui sont, soit un concurrent d'Infor, soit non suffisamment qualifiés ou indépendants). Le Client convient que l'audit sera effectué sans interférer de manière déraisonnable avec les activités commerciales d'Infor (ou de ses sous-traitants), pendant les heures de bureau régulières avec un préavis raisonnable, et soumis aux politiques de sécurité applicables et aux procédures de confidentialité d'Infor (ou de ses sous-traitants). Lorsque les audits sur site des centres de données physiques, des systèmes ou des installations ne sont pas autorisés, Infor collaborera avec le Client (et ses sous-traitants, le cas échéant) pour parvenir à une résolution mutuellement acceptable suffisante pour fournir les informations nécessaires au Client pour se conformer aux exigences d'audit en vertu du Droit Applicable en matière de Cybersécurité et de Gouvernance des Données. Ni le Client, ni l'auditeur, n'auront accès à des données d'autres clients d'Infor ou aux systèmes ou installations d'Infor non impliqués dans les Services fournis au Client. Le Client devra fournir les

résultats de tout audit à Infor. Les parties s'accorderont mutuellement sur tous les rapports ou mesures correctives correspondants. Infor fera des efforts commerciaux raisonnables pour traiter les mesures correctives convenues.

7.5 Le Client est responsable de tous les coûts et frais liés à l'audit, y compris tous les coûts et frais raisonnables qu'Infor engage pour l'audit et tous les coûts et frais qu'Infor engage auprès de tout sous-traitant lorsque l'audit implique un sous-traitant, sauf si cet audit révèle une violation matérielle par Infor de la présente Annexe, auquel cas Infor supportera ses propres dépenses pour cette partie de l'audit liée à la violation.

III. DORA

1. PÉRIMÈTRE ET DÉFINITIONS

1.1 Les termes et conditions énoncés dans la Section III de la présente Annexe s'appliquent uniquement aux Clients de l'UE qui répondent aux critères et seuils pour les entités financières régulées par DORA. Pour éviter toute ambiguïté, la Section I est réputée incorporée à cette Section III ; des paragraphes spécifiques de la Section II s'appliquent également s'ils sont spécifiquement référencés dans cette Section III.

1.2 « **DORA** » désigne le Règlement sur la Résilience Opérationnelle Numérique (Règlement (UE) 2022/2554 du Parlement Européen et du Conseil du 14 décembre 2022).

2. SERVICES

2.1 Le Service TIC fourni par Infor au Client est décrit dans les Contrats.

3. EMPLACEMENT

3.1 Pour éviter toute ambiguïté, les données de production du Client sont stockées dans l'emplacement de déploiement sélectionné et Infor ne déplacera aucune des données de production du Client en dehors de cet emplacement sans l'approbation écrite préalable et la direction du Client. À la direction du Client, des quantités limitées de données personnelles peuvent être accessibles à distance depuis l'extérieur de l'emplacement de déploiement sélectionné aux fins de fournir un support et des services au Client. Infor notifiera au Client à l'avance s'il envisage de modifier les emplacements (c'est-à-dire les régions ou pays) où les Services seront fournis et où les Données Client seront stockées et traitées, comme indiqué dans les Contrats.

4. PROGRAMME DE SÉCURITÉ ET SLA

4.1 Les mesures de gestion des risques de cybersécurité décrites ci-dessus dans la Section II.3 et Section II.4 s'appliquent. Les engagements de réponse aux incidents d'Infor dans la Section II.6 s'appliquent également. Pour éviter toute ambiguïté, l'insolvabilité d'Infor est considérée comme ajoutée en tant qu'obligation de restitution des Données Client en vertu du PSI.

4.2 Les engagements de disponibilité au niveau des services d'Infor sont décrits dans l'Accord de Niveau de Service à l'adresse https://www.infor.com/service-level-description (« SLA »). Les engagements de support spécifiques aux produits sont décrits dans le Bon de Commande, le cas échéant.

5. FORMATION À LA SÉCURITÉ TIC ET PROGRAMMES DE SENSIBILISATION

5.1 Si Infor accède aux systèmes d'information du réseau sur site du Client dans le cadre des Services, le Client peut demander à Infor de participer, moyennant un préavis raisonnable, à tout programme approprié de sensibilisation à la sécurité TIC et/ou formation à la résilience opérationnelle numérique que le Client fournit ou exploite en relation avec son entreprise (« Formation »). À cet égard, les parties conviennent que :

(A) La fréquence, le calendrier et la durée de cette Formation seront convenus par les parties à l'avance ;

(B) Infor se réserve le droit de récupérer auprès du Client ses dépenses raisonnables et dûment engagées ; et

(C) La participation d'Infor à cette Formation ne doit pas l'obliger à faire quoi que ce soit qui pourrait interférer, empêcher ou entraver Infor de fournir les Services TIC ou autrement d'exécuter ses obligations en vertu des Contrats.

6. RÉSILIATION

6.1 En plus des droits de résiliation énoncés dans les Contrats et ailleurs dans les présentes conditions générales, comme autorisé par l'Art. 28 Section 7 de DORA et sous réserve du processus de résiliation dans les Contrats, le Client peut résilier les Contrats dans son intégralité ou en partie uniquement dans les cas suivants : (i) si Infor n'a pas remédié à une violation significative du Droit Applicable en matière de Cybersécurité et de Gouvernance des Données ou de la présente Annexe, (ii) si des circonstances sont identifiées par le Client qui sont jugées capables de modifier la performance par Infor des Services TIC, y compris des changements matériels qui affectent les Contrats ou la situation d'Infor, (iii) si des faiblesses évidentes sont constatées concernant la gestion globale des risques TIC d'Infor et en particulier la manière dont Infor assure la disponibilité, l'authenticité, l'intégrité et la confidentialité des données, qu'il s'agisse de données personnelles ou d'autres données sensibles, ou de données non personnelles, ou (iv) si l'autorité gouvernementale compétente ne peut plus superviser efficacement le Client en raison des conditions de, ou des circonstances liées à, Infor ou aux Contrats.

7. INTERACTIONS AVEC LES AUTORITÉS GOUVERNEMENTALES COMPÉTENTES

7.1 Infor coopérera pleinement avec les autorités gouvernementales compétentes et les autorités de résolution du Client, y compris les personnes désignées par elles.