

MODALITÉS DU FOURNISSEUR RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET À LA SÉCURITÉ

Ces Modalités relatives à la protection des renseignements personnels et à la sécurité établissent les droits et les obligations de Kyndryl et du Fournisseur concernant la régie des données, la sécurité et les sujets connexes (les « **Modalités** »). Les Modalités sont incorporées dans le Contrat de relation Fournisseur (ou accord équivalent) entre les parties, y compris les Énoncés des travaux, les Autorisations de travail ou d'autres documents entre nos entreprises qui s'y réfèrent (les « **Documents transactionnels** ») et en font partie intégrante.

Les présentes Modalités comprennent :

- Ce document,
- L'Annexe relative aux détails du traitement jointe au présent document décrit les activités de traitement de données du Fournisseur à compter de l'exécution des présentes Modalités (pour tout document transactionnel conclu après l'exécution des présentes Modalités, une Annexe sur les détails du traitement distincte sera jointe à chaque document transactionnel, documentant les activités de traitement du Fournisseur spécifiques à ce document), et
- Les Clauses contractuelles types de l'UE, l'Addendum concernant le transfert de données international du Royaume-Uni et l'Évaluation de l'impact du transfert des fournisseurs sont disponibles à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.

En cas d'incompatibilité entre les dispositions des présentes Modalités, le Contrat de relation Fournisseur, un accord équivalent ou un Document transactionnel, y compris tout accord de traitement de données, les présentes Modalités prévaudront. En cas d'incompatibilité entre les présentes Modalités et les dispositions mutuellement convenues entre le Fournisseur et Kyndryl pour un Client Kyndryl, les dispositions mutuellement convenues pour un Client Kyndryl prévaudront.

Les mots commençant par une majuscule ont la signification qui leur est donnée dans l'Article V de ces Modalités, dans les autres dispositions des présentes Modalités, dans un Document transactionnel ou un contrat de base connexe conclu entre les parties.

Article I. RÉGIE DES DONNÉES ET IA

1.1. **Conformité aux lois.** Le Fournisseur se conformera à toutes les lois qui s'appliquent aux Services et aux Produits et services livrables, y compris aux lois relatives à protection des données, à la cybersécurité et aux systèmes d'IA. Le Fournisseur informera rapidement Kyndryl (dans les délais imposés par la loi et en permettant à Kyndryl de respecter ses propres obligations juridiques), si le Fournisseur détermine qu'il ne peut plus remplir ses obligations juridiques.

1.2. **Utilisation des données.** Le Fournisseur ne doit pas :

- (a) utiliser les Données Kyndryl sous quelque forme que ce soit, y compris sous forme agrégée, anonymisée ou autre, à d'autres fins que la fourniture des Services et des Produits et services livrables (à titre d'exemple, le Fournisseur n'est pas autorisé à utiliser ou à réutiliser les Données Kyndryl pour évaluer l'efficacité ou les moyens d'améliorer les offres du Fournisseur autres que les Services ou les Produits et services livrables, à des fins de recherche et développement pour créer de nouvelles offres, ou pour générer des rapports concernant les offres du Fournisseur)
- (b) Vendre ou partager les Données Kyndryl; ou
- (c) tenter de ré-identifier toute information qui peut raisonnablement servir à déduire des informations sur une Personne concernée ou être autrement liée à celle-ci.

1.3. **Technologies de suivi Web.** Si le Fournisseur ou ses Sous-traitants, dans le cadre de la fourniture des Services ou des Produits et services livrables, recueillent des données à l'aide de technologies de suivi Web (y compris le HTML5, le stockage local, les balises ou les jetons tiers et les balises Web), ces données sont considérées comme des données Kyndryl et le Fournisseur se conformera à ses obligations concernant les Données Kyndryl en vertu des présentes Modalités.

- 1.4. **Non-divulgation.** Le Fournisseur ne divulguera pas les Données de Kyndryl à des tiers, autre qu'aux sous-traitants ultérieurs approuvés conformément à la Section 2.5 ou aux sous-traitants approuvés conformément à l'Accord.
- 1.5. **Accès par le gouvernement.** Si un gouvernement, y compris tout responsable de la réglementation, demande l'accès aux données Kyndryl (p. ex., si le gouvernement américain ordonne au Fournisseur de divulguer des Données de Kyndryl pour des raisons de sécurité nationale), ou si une divulgation des Données Kyndryl est autrement requise par la loi, le Fournisseur informera rapidement Kyndryl par écrit de cette demande ou de cette exigence et offrira à Kyndryl une occasion raisonnable de contester toute divulgation, sauf si la loi l'interdit. Si la loi interdit une telle notification, le Fournisseur prendra les mesures qu'il estime raisonnablement appropriées pour contester l'interdiction et la divulgation des Données Kyndryl par le biais d'une action judiciaire ou d'autres moyens.
- 1.6. **Confidentialité des données.** Le Fournisseur confirme à Kyndryl que : (a) seuls ses employés qui doivent accéder aux Données Kyndryl pour fournir des Services ou des Produits et services livrables y auront accès, et uniquement dans la mesure où cela est nécessaire; et (b) ses employés sont liés par des obligations de confidentialité des données qui les obligent à utiliser et à divulguer les Données Kyndryl uniquement dans la mesure où les présentes Modalités le permettent.
- 1.7. **Restitution ou suppression des Données Kyndryl.** À la demande de Kyndryl, le Fournisseur supprimera ou restituera à ses frais les Données Kyndryl dès la résiliation ou l'expiration du Document transactionnel ou plus tôt, si Kyndryl le demande. Si Kyndryl en exige la suppression, le Fournisseur rendra les Données illisibles et impossibles à réassembler ou à reconstituer, conformément à la publication spéciale 800-88 rév.1 du National Institute of Standards and Technology (NIST), et en certifiera la suppression à Kyndryl. Si Kyndryl exige la restitution des données Kyndryl, le Fournisseur le fera dans un format couramment utilisé en respectant les délais et les instructions raisonnables de Kyndryl.
- 1.8. **Systèmes d'IA**
- (a) Le Fournisseur ne doit pas utiliser de systèmes d'IA dans la fourniture de Services ou de Produits et services livrables, ni inclure de systèmes d'IA dans un Produit ou service livrable, sans l'autorisation préalable de Kyndryl figurant dans un Document transactionnel ou dans l'Accord. En demandant l'autorisation de Kyndryl, le Fournisseur fournira à Kyndryl par écrit toutes les informations nécessaires pour évaluer l'utilisation des systèmes d'IA par le Fournisseur (p. ex., les flux de données, les modèles de langage utilisés, la séparation des données).
 - (b) Le Fournisseur déclare et garantit que : (i) les intrants fournis par Kyndryl (y compris les intrants fournis par les employés ou par tout autre tiers en vertu d'un Document transactionnel) et les extrants seront classés comme étant des Œuvres de Kyndryl, (ii) le Fournisseur n'utilisera pas les Œuvres de Kyndryl pour entraîner ou pour peaufiner le modèle de base ou d'autres éléments des Systèmes d'IA, (iii) le Fournisseur ne sauvegardera pas les Œuvres de Kyndryl plus longtemps que nécessaire pour fournir les Services, (iv) les Systèmes d'IA (y compris les extrants et les données d'entraînement) seront classés comme faisant partie des Services, et (v) dans la mesure permise par loi en vigueur, le Fournisseur cède par la présente tous ses droits, ses titres et ses intérêts relatifs aux extrants des Systèmes d'IA à Kyndryl.
 - (c) Le Fournisseur doit mettre en place et tenir à jour un programme documenté de gouvernance et de gestion de risques pour les systèmes d'IA qui identifie, teste, surveille et réduit de manière raisonnable et appropriée les risques connus et prévisibles, y compris, sans s'y limiter, les risques liés à l'éthique, aux biais, à la sécurité et à la sûreté associés aux systèmes d'IA ou découlant de ceux-ci. Sur demande, le Fournisseur fournira une copie de son programme de gouvernance et de gestion de risques pour les systèmes d'IA. Le Fournisseur informera rapidement Kyndryl par écrit de tout risque survenu ou de tout risque important identifié conformément à la disposition de notification convenue dans le document transactionnel en envoyant une copie à ailegalteam@kyndryl.com.

Article II. PROTECTION DES RENSEIGNEMENTS PERSONNELS

- 2.1. **Coordonnées professionnelles.** Kyndryl et le Fournisseur peuvent traiter les coordonnées professionnelles (BCI) de l'autre conformément aux lois en vigueur relatives à la protection des données en tant que Responsables du traitement indépendants partout où ils mènent des activités pour livrer et recevoir les Produits et services livrables

et les Services. Les parties n'agissent pas en tant que co-responsables du traitement à l'égard des BCI de l'autre. Si l'une des parties informe l'autre de toute demande d'une Personne concernée relative aux BCI de l'autre, l'autre partie aura la responsabilité de répondre à ces demandes directement auprès de la Personne concernée. Chacune des parties a mis en œuvre des mesures techniques et organisationnelles appropriées pour protéger les BCI de l'autre. Par souci de clarté, la Section 3.12 (Incidents de sécurité) s'applique aux BCI.

2.2. Fournisseur en tant que sous-traitant. Kyndryl désigne le Fournisseur en tant que sous-traitant chargé du traitement des Données à caractère personnel de Kyndryl dans le seul but de fournir les Produits et services livrables et les Services conformément aux instructions de Kyndryl, y compris celles contenues dans les présentes Modalités, l'Accord et tout document transactionnel connexe. Le Fournisseur est un sous-traitant chargé du traitement des Données à caractère personnel de Kyndryl. Si le Fournisseur n'agit pas conformément aux instructions de Kyndryl afin que Kyndryl puisse se conformer à la loi applicable en matière de protection des données, Kyndryl peut mettre fin à la partie concernée des Services moyennant un avis écrit. Si le Fournisseur estime qu'une instruction enfreint une loi sur la protection des données, il doit en informer Kyndryl rapidement et en respectant tout délai exigé par la loi.

2.3. Mesures techniques et organisationnelles. Le Fournisseur mettra en place et tiendra à jour des mesures techniques et organisationnelles appropriées, y compris les mesures de sécurité visées à l'Article III ci-dessous, afin d'assurer un niveau de sécurité adapté au risque associé à la fourniture des Services et des Produits et services livrables.

2.4. Droits et demandes des personnes concernées

- (a) Le Fournisseur informera rapidement Kyndryl (c.-à-d., dans un délai qui permet à Kyndryl et à tout autre Responsable du traitement de s'acquitter de leurs obligations juridiques) des demandes qu'il reçoit de Personnes concernées pour exercer leurs droits (notamment, concernant la rectification, la suppression ou le blocage de Données) à l'égard des Données à caractère personnel de Kyndryl. Le Fournisseur peut également diriger rapidement une personne concernée faisant une telle requête vers Kyndryl. Le Fournisseur ne répondra à aucune demande des personnes concernées, à moins que la loi ne l'y oblige ou que Kyndryl ne lui donne des instructions écrites à cet effet.
- (b) Si Kyndryl est obligée de fournir de l'information relative à des Données à caractère personnel de Kyndryl à d'autres Responsables du traitement ou à des tiers (p. ex., à des Personnes concernées ou des responsables de la réglementation), le Fournisseur offrira immédiatement son assistance à Kyndryl en lui fournissant l'information et en prenant toute mesure raisonnable demandée par Kyndryl, dans un délai qui permet à Kyndryl de répondre en temps opportun aux autres responsables du traitement ou aux tiers.

2.5. Sous-traitants ultérieurs

- (a) Kyndryl autorise le Fournisseur à faire appel aux sous-traitants ultérieurs répertoriés dans les Annexes relatives aux détails du traitement respectives. Le Fournisseur peut également engager des sous-traitants ultérieurs supplémentaires ou de remplacement, ou élargir la portée du traitement effectué par un sous-traitant ultérieur existant, sous réserve des conditions suivantes :
 - (i) Le Fournisseur remettra à Kyndryl un préavis écrit avant de procéder à de tels changements.
 - (ii) Kyndryl peut s'opposer à l'ajout d'un nouveau sous-traitant ultérieur ou au remplacement d'un sous-traitant ultérieur existant ou à l'élargissement de sa portée, et les parties travailleront ensemble de bonne foi en vue de s'entendre sur ce sujet.
 - (iii) Sous réserve du droit à l'objection de Kyndryl à tout moment, le Fournisseur peut procéder au changement, si Kyndryl n'a pas soulevé d'objection dans les 30 jours suivant la réception de l'avis écrit du Fournisseur.
- (b) Le Fournisseur soumettra chaque sous-traitant ultérieur agréé aux obligations de protection des données, de sécurité et de certification énoncées dans les présentes Modalités, avant qu'un sous-traitant ultérieur ne puisse traiter des données à caractère personnel de Kyndryl. Le Fournisseur est entièrement responsable envers Kyndryl du respect de ces obligations par chaque sous-traitant ultérieur.

2.6. Traitement des données transfrontalier

- (a) Le Fournisseur ne transférera ni ne divulguera (y compris par accès à distance) aucune Donnée à caractère personnel de Kyndryl au-delà des frontières, sauf à des sous-traitants ultérieurs approuvés conformément à

la Section 2.5. Si Kyndryl approuve le transfert transfrontalier des Données à caractère personnel de Kyndryl, les parties coopéreront pour se conformer aux lois applicables en matière de protection des données. Si ces lois exigent l'utilisation de Clauses contractuelles types, le Fournisseur acceptera rapidement lesdites Clauses telles que définies ci-dessous.

(b) **Espace économique européen**

- (i) Si Kyndryl transfère des Données à caractère personnel soumises au Règlement général sur la protection des données (2016/679) en dehors de l'Espace économique européen à un Fournisseur non établi dans un Pays adéquat, le Fournisseur adhère par la présente aux Clauses contractuelles types de l'UE (Décision 2021/914 de la Commission), pré-signées par Kyndryl et disponibles à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> (« CCT de l'UE »).
- (ii) Dans le cas où Kyndryl aurait effectivement disparu, cessé d'exister en droit ou serait devenu insolvable, les autres Responsables du traitement auront le droit de résilier l'Accord et de demander au Fournisseur d'effacer ou de restituer les données à caractère personnel de Kyndryl.
- (iii) L'évaluation de Kyndryl des transferts de Données à caractère personnel aux Fournisseurs comme l'exigent les Clauses contractuelles types de l'UE est publiée aux fins d'examen par le Fournisseur à l'adresse <https://www.kyndryl.com/us/en/procurement/terms/privacy-and-security-terms>.
- (iv) Le Fournisseur fournira suffisamment de détails sur chaque sous-traitant ultérieur dans les avis et les Annexes relatives aux Détails du traitement pour satisfaire à ses obligations en tant qu'importateur de données en vertu de la clause 14(c) des Clauses contractuelles types de l'UE, y compris le nom du sous-traitant ultérieur, les lieux du traitement et les activités de traitement.
- (v) Le Fournisseur agira en tant qu'exportateur de données et adhère aux Clauses contractuelles types de l'UE ou tout autre mécanisme de transfert approprié avec chaque sous-traitant ultérieur approuvé qui n'est pas établi dans un Pays adéquat.

(c) **Royaume-Uni.** Si les Données à caractère personnel de Kyndryl soumises à la loi du Royaume-Uni sur la protection des données (2018) sont transférées en dehors du Royaume-Uni vers un Pays non adéquat, le Fournisseur adhère par la présente à l'Addendum sur le transfert de données international du Royaume-Uni, pré-signé par Kyndryl et disponible à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.

(d) **Suisse.** Si les Données à caractère personnel de Kyndryl soumises à la loi fédérale de la Suisse sur la protection des données (« FADP ») sont transférées hors de la Suisse vers un Pays non adéquat, le Fournisseur adhère par la présente aux Clauses contractuelles types de l'UE, sous réserve des modifications suivantes :

- (i) les références au RGPD doivent également inclure la référence aux dispositions équivalentes de la FADP;
- (ii) la Commission fédérale suisse sur la protection des données est l'autorité de contrôle exclusive conformément à la Clause 13 et à l'Annexe I.C des Clauses contractuelles types de l'UE;
- (iii) la loi applicable conformément à la Clause 17 des Clauses contractuelles types de l'UE est le droit suisse si le transfert de données est exclusivement soumis à la loi FADP; et
- (iv) le terme « État membre » ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité de faire valoir leurs droits dans leur lieu de résidence habituelle (Suisse) conformément à la Clause 18 des Clauses contractuelles types de l'UE.

(e) **Brésil.** Si Kyndryl transfère des Données à caractère personnel soumises à la Lei Geral de Proteção de Dados (LGPD) hors du Brésil à un Fournisseur non établi dans un Pays adéquat, le Fournisseur s'engage par la présente à respecter l'Annexe II de la Resolução CD/ANPD n° 19/2024 (ci-après les « Clauses contractuelles types du Brésil » ou « CCT du Brésil »), préalablement signée par Kyndryl et disponible à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> (« CCT du Brésil »).

(f) **Autres pays.** Si un transfert de Données à caractère personnel de Kyndryl est soumis aux lois sur la protection des données d'un pays où les Clauses contractuelles types locales n'ont pas été publiées par l'Autorité de contrôle (p. ex., la loi péruvienne sur la protection des données, la loi sud-africaine sur la protection des données) ou si l'Autorité de contrôle a approuvé l'utilisation des Clauses contractuelles types de l'UE comme mesure de sauvegarde suffisante pour le transfert transfrontalier (p. ex., la loi argentine sur la protection des données), les Clauses contractuelles types de l'UE régiront ce transfert sous réserve des modifications suivantes :

- (i) les références au RGPD doivent également inclure la référence aux dispositions équivalentes de la loi sur la protection des données;
- (ii) l'autorité de contrôle de l'État local est l'autorité de contrôle exclusive conformément à la Clause 13 et à l'Annexe I.C des Clauses contractuelles types de l'UE;

- (iii) la loi applicable conformément à la Clause 17 des Clauses contractuelles types de l'UE sera la loi locale sur la protection des données; et
- (iv) le terme « État membre » ne doit pas être interprété de manière à exclure les personnes concernées dans le pays de la possibilité de faire valoir leurs droits dans leur lieu de résidence habituelle conformément à la Clause 18 des Clauses contractuelles types de l'UE.

2.7. Assistance et registres

- (a) Selon la nature du Traitement, le Fournisseur aidera Kyndryl en mettant en place les Mesures techniques et organisationnelles appropriées (« **TOM** ») pour remplir les obligations associées aux demandes et aux droits des Personnes concernées. Le Fournisseur aidera également Kyndryl à assurer le respect des obligations concernant la sécurité du traitement, la notification et la communication d'un incident relatif à la sécurité et la création d'une analyse d'impact sur la protection des Données, y compris la consultation préalable auprès du responsable de la réglementation pertinent, si nécessaire, en tenant compte de l'information qui est à la disposition du Fournisseur.
- (b) Le Fournisseur tiendra à jour dans un registre contenant le nom et les coordonnées de chaque sous-traitant ultérieur, y compris du représentant et du délégué à la protection des données de chaque sous-traitant ultérieur. Le Fournisseur remettra ce registre à Kyndryl sur demande, dans un délai qui permettra à Kyndryl de répondre en temps opportun à une demande d'un Client ou d'un tiers.

2.8. Modalités nationales requises

(a) Japon

- i) Pour les Coordonnées professionnelles des Personnes concernées situées au Japon, le Fournisseur se conformera aux dispositions des présentes Modalités, applicables au Fournisseur en tant que sous-traitant.
- ii) La définition du terme « Incident relatif à la sécurité » dans les présentes Modalités est par la présente modifiée pour inclure les violations raisonnablement suspectées des Données à caractère personnel de Kyndryl liées aux Personnes concernées situées au Japon.
- iii) Le Fournisseur garantit qu'il n'a aucune raison de croire que les lois et les pratiques de tout pays dans lequel le Fournisseur ou ses sous-traitants ultérieurs traiteront les Données à caractère personnel de Kyndryl empêchent le Fournisseur de remplir ses obligations en vertu des présentes Modalités. Le Fournisseur informera Kyndryl si, après avoir accepté les Modalités et pendant la durée des Modalités, le Fournisseur a des raisons de croire qu'il ne peut pas se conformer à ses obligations en vertu des Modalités. Dans ce cas, les parties coopéreront de bonne foi pour identifier les mesures appropriées à adopter pour remédier à la situation. Si aucune mesure appropriée ne peut être mise en œuvre, Kyndryl évaluera s'il convient de suspendre le transfert des Données à caractère personnel de Kyndryl.

- (b) **Californie.** Lorsque le Fournisseur, en tant que sous-traitant, traite les Données à caractère personnel de Kyndryl de Personnes concernées situées dans l'État de Californie, (i) Kyndryl divulgue les Données à caractère personnel de Kyndryl au Fournisseur uniquement aux fins commerciales limitées et spécifiées sélectionnées dans l'Annexe relative aux détails du traitement applicable, (ii) Kyndryl peut, sur préavis, prendre des mesures raisonnables et appropriées pour mettre fin au Traitement non autorisé ou pour s'assurer que le Traitement du Fournisseur est conforme aux obligations de Kyndryl en vertu des lois applicables en matière de protection des données, et (iii) le Fournisseur ne conservera, n'utilisera ni ne divulguera les Données à caractère personnel de Kyndryl en dehors des relations commerciales directes entre Kyndryl et le Fournisseur.

(c) Canada.

- i) Pour les Coordonnées professionnelles des Personnes concernées situées au Canada, le Fournisseur se conformera aux dispositions des présentes Modalités, applicables au Fournisseur en tant que sous-traitant, dans la mesure où ces données sont considérées comme des Données à caractère personnel.
- ii) Pour plus de clarté, les références aux lois applicables en matière de protection des données comprennent, sans s'y limiter, toutes les directives juridiquement contraignantes et les bonnes pratiques publiées par une Autorité de contrôle compétente au Canada, telles que modifiées, remplacées ou abrogées.
- iii) Le Fournisseur n'utilisera pas les Données de Kyndryl pour créer une base de données de caractéristiques biométriques et/ou des mesures à des fins d'identification personnelle.
- iv) Le Fournisseur effectuera toute évaluation d'impact sur la protection des renseignements personnels ou évaluation d'impact sur le transfert requise en vertu des lois sur la protection des données du Canada,

- fournira une copie de ces évaluations sur demande, et avisera Kyndryl dans les meilleurs délais de toute mesure supplémentaire à appliquer.
- v) Dans le cas où Kyndryl n'est pas d'accord avec les résultats des évaluations ou des mesures supplémentaires du Fournisseur, Kyndryl et le Fournisseur travailleront ensemble pour trouver une solution viable. Si les Parties ne parviennent pas à s'entendre sur une solution viable, Kyndryl se réserve le droit de suspendre ou de résilier les services concernés du Fournisseur sans indemnisation.
 - vi) Le Fournisseur aidera Kyndryl en fournissant les informations supplémentaires raisonnablement demandées pour permettre à Kyndryl de mener sa propre évaluation, conformément aux lois canadiennes applicables en matière de protection des données, afin de déterminer si les Modalités offrent une protection adéquate.

Article III. SÉCURITÉ GÉNÉRALE

3.1. Procédures de sécurité

- (a) **Procédures.** Les procédures de sécurité de l'information du Fournisseur seront documentées, approuvées par la haute direction du Fournisseur et conformes aux pratiques normalisées de l'industrie telles que celles du National Institute of Standards and Technology (NIST) et/ou de l'Organisation internationale de normalisation (ISO). Les procédures de sécurité de l'information du Fournisseur seront examinées et évaluées par le Fournisseur au moins une fois par an, et dès que des modifications importantes y seront apportées, afin de confirmer qu'elles restent applicables et efficaces. Le Fournisseur n'apportera pas de modifications aux procédures susceptibles de compromettre la sécurité du Fournisseur en ce qui concerne les Œuvres, les Produits et services livrables ou les Services Kyndryl.
- (b) **Tests.** Le Fournisseur tiendra à jour un processus permettant de tester régulièrement l'efficacité de ses mesures techniques et organisationnelles pour assurer la sécurité des Œuvres, des Produits et services livrables et des Services Kyndryl.
- (c) **Gestion des risques.** Le Fournisseur effectuera des évaluations appropriées des risques de sécurité de l'information dans le cadre d'un programme continu de gouvernance des risques avec les objectifs suivants :
 - (i) identifier les risques de sécurité de l'information liés aux Œuvres, aux Produits et services livrables et aux Services Kyndryl; (ii) évaluer l'impact de ces risques; et (iii) lorsque des stratégies de réduction ou d'atténuation des risques sont identifiées ou justifiées, mettre en place des mesures pour atténuer et gérer efficacement ces risques, en tenant compte du fait que les menaces évoluent constamment.

3.2. Sécurité du personnel

- (a) **Formation en sécurité.** Le Fournisseur dispensera au moins une fois par an une formation de sensibilisation à la sécurité et à la protection des renseignements personnels à l'ensemble du personnel du Fournisseur ayant accès ou pouvant avoir accès aux Œuvres, aux Produits et services livrables ou aux Services Kyndryl.
- (b) **Vérification des antécédents.** Le Fournisseur tiendra à jour et suivra des exigences de vérification d'emploi normalisées et obligatoires pour tous les nouveaux employés, et imposera ces exigences à l'ensemble du personnel du Fournisseur et du personnel des filiales contrôlées par le Fournisseur. Ces exigences incluront une vérification des antécédents criminels, dans la mesure permise par les lois locales, la validation d'une preuve d'identité, ainsi que d'autres vérifications que le Fournisseur juge nécessaires. Le Fournisseur répétera et revalidera périodiquement ces activités de vérification, comme il le juge nécessaire.

3.3. Gestion des biens

- (a) **Inventaire des biens.** Le Fournisseur tiendra à jour un inventaire des biens de tous les équipements sur lesquels les Œuvres Kyndryl sont stockées. Le Fournisseur limitera l'accès à cet équipement uniquement au Personnel autorisé du Fournisseur. Le Fournisseur empêchera l'accès non autorisé ainsi que la copie, la modification ou la suppression des Œuvres Kyndryl. Le Fournisseur tiendra à jour des mesures pour empêcher l'accès, la copie, la modification ou la suppression non autorisés des Œuvres Kyndryl.
- (b) **Sécurité des éléments logiciels.** Le Fournisseur s'engage à faire l'inventaire approprié de tous les éléments logiciels (y compris les logiciels à source ouverte) utilisés dans la fourniture des Services et dans le développement et la fourniture des Produits et services livrables. Le Fournisseur évaluera si ces éléments logiciels présentent des anomalies de sécurité et/ou des vulnérabilités qui pourraient entraîner la divulgation ou l'accès non autorisé aux Œuvres, aux Produits et services livrables ou aux Services Kyndryl. Le Fournisseur effectuera cette évaluation avant de livrer les Services et les Produits et services livrables ou d'en permettre l'accès à Kyndryl de manière continue par la suite pendant la durée déterminée dans le Document

transactionnel. Le Fournisseur s'engage à remédier en temps opportun à toute anomalie de sécurité ou vulnérabilité dans tout élément logiciel dont le Fournisseur prend connaissance. Le Fournisseur répondra rapidement à toute demande de Kyndryl visant à savoir si une anomalie ou une vulnérabilité de sécurité dans un tel élément logiciel est connue du Fournisseur et/ou a été corrigée par le Fournisseur.

3.4. Politique de contrôle d'accès. Le Fournisseur tiendra à jour une politique de contrôle d'accès basé sur les rôles et des mesures techniques de contrôle d'accès appropriées conformément aux pratiques normalisées de l'industrie pour restreindre l'accès aux Œuvres Kyndryl et aux biens du Fournisseur utilisés pour fournir les Services uniquement au Personnel autorisé du Fournisseur et limiter cet accès au niveau le plus bas requis pour fournir et soutenir les Services et les Produits et services livrables. Ces accès seront consignés conformément aux exigences énumérées sous 3.10(f).

3.5. Autorisation

- (a) Le Fournisseur tiendra à jour des procédures de création et de suppression de comptes d'utilisateur pour accorder et révoquer rapidement (et dans tous les cas dans les vingt-quatre (24) heures) l'accès à toutes les Œuvres Kyndryl et à toutes les applications et biens internes du Fournisseur utilisés dans la fourniture des Services et des Produits et services livrables. Le Fournisseur attribuera une autorisation appropriée pour approuver la création et la révocation de comptes d'utilisateur ou des niveaux d'accès élevés ou réduits pour les comptes existants, y compris lors de la cessation d'un emploi, d'un contrat, d'un engagement ou de tout autre accord avec le Fournisseur ou une modification de rôle si ce membre du Personnel n'a plus besoin de ces droits accès.
- (b) Le Fournisseur tiendra à jour les registres du Personnel du Fournisseur qui est autorisé à accéder aux systèmes et aux biens sur lesquels sont stockés ou à partir desquels peuvent être consultés les Œuvres Kyndryl et les Produits et services livrables ou qui sont utilisés pour fournir les Services et effectuera des contrôles périodiques de ces registres au moins une fois par trimestre. Le personnel de l'administration et de l'assistance technique ne sera autorisé à accéder à ces systèmes, aux Œuvres et aux Produits et services livrables Kyndryl que lorsque cela est nécessaire et à condition que ce Personnel se conforme aux mesures techniques et organisationnelles applicables du Fournisseur.
- (c) Le Fournisseur s'assurera que les comptes d'utilisateur ayant accès à ces systèmes et à ces biens sont uniques et contrôlés par mot de passe et que les comptes d'utilisateur ne sont pas partagés.

3.6. Authentification

- (a) Le Fournisseur effectuera une surveillance pour déceler toute tentative accès répétée aux systèmes d'information et aux biens.
- (b) Le Fournisseur tiendra à jour des pratiques de protection par mot de passe qui sont conformes aux pratiques normalisées de l'industrie et conçues pour préserver la confidentialité et l'intégrité des mots de passe générés, attribués, distribués et stockés sous quelque forme que ce soit. Le Fournisseur générera ou demandera à l'utilisateur de créer et d'utiliser un mot de passe ou une phrase de passe complexe générée(e) aléatoirement ou des alternatives appropriées, telles que des certificats numériques, des cartes / des jetons matériels ou la biométrie.
- (c) Le Fournisseur utilisera l'authentification multifactorielle, y compris pour l'accès administratif au domaine et au portail infonuagique. L'authentification multifactorielle peut inclure des techniques telles que l'utilisation de certificats cryptographiques, de jetons à mot de passe à usage unique (OTP) ou la biométrie.

3.7. Cryptographie

- (a) **Politique.** Le Fournisseur mettra en place et tiendra à jour des procédures et des normes cryptographiques conformes aux pratiques normalisées de l'industrie pour protéger les Œuvres Kyndryl, y compris, le cas échéant, la pseudonymisation et le chiffrement.
- (b) **Chiffrement** Le Fournisseur doit chiffrer les Œuvres Kyndryl en transit et au repos. Les algorithmes de chiffrement protégeront les données à des niveaux de sécurité conformes aux pratiques normalisées de l'industrie (telles que NIST SP 800-131a) et utiliseront des fonctions de hachage reconnues dans l'industrie, qui assureront une protection au moins égale à celle du chiffrement Advanced Encryption Standard 256 bits (AES 256) au repos et à celle de TLS v1.2 en transit. Le Fournisseur tiendra à jour et respectera des procédures et des pratiques gestion des clés conformément aux pratiques normalisées de l'industrie, qui définissent les exigences, la sécurité, la rotation et le cycle de vie des clés de chiffrement, y compris la création, la distribution, la révocation, l'archivage et la destruction.

3.8. Sécurité physique et environnementale

- (a) **Accès aux installations.** Le Fournisseur limitera l'accès aux installations à son Personnel autorisé.
- (b) **Protection contre les interruptions.** Le Fournisseur déploiera des efforts raisonnables pour protéger ces systèmes et ces biens contre les pannes de courant et autres interruptions causées par des pannes des services publics.
- (c) **Élimination ou réutilisation sécurisée de l'équipement.** Le Fournisseur s'assurera que toutes les Œuvres Kyndryl ont été supprimées ou écrasées en toute sécurité des équipements contenant des supports de stockage à l'aide de processus conformes aux pratiques normalisées de l'industrie avant l'élimination ou la réutilisation de ces équipements.

3.9. Sécurité des opérations

- (a) **Politique des opérations.** Le Fournisseur tiendra à jour des procédures opérationnelles et de sécurité appropriées qui seront mises à la disposition de tout le Personnel qui en a besoin.
- (b) **Protections contre les maliciels.** Le Fournisseur déploiera des solutions antivirus et de gestion des terminaux pour mettre en place des contrôles anti-maliciels afin de protéger ces systèmes et ces biens contre les logiciels malveillants, y compris ceux qui proviennent de réseaux publics.
- (c) **Gestion de la configuration.** Le Fournisseur disposera de procédures régissant l'installation de logiciels et d'utilitaires par le Personnel.
- (d) **Gestion des changements.** Le Fournisseur tiendra à jour et mettra en œuvre des procédures pour garantir que seules les versions approuvées et sécurisées du code, des configurations, des systèmes et des applications seront déployées dans les environnements de production.
- (e) **Séparation logique.** Le Fournisseur veillera à isoler de manière adéquate ses environnements de production, hors production et autres environnements. Si des Œuvres Kyndryl sont déjà présentes dans un environnement hors production ou y sont transférés (p. ex., pour reproduire une erreur), le Fournisseur s'assurera que toutes les mesures de sécurité et de confidentialité dans l'environnement hors production sont équivalentes à celles qui sont utilisées en environnement de production.

3.10. Sécurité des communications

- (a) **Transfert d'informations.** Le Fournisseur limitera l'accès par chiffrement aux Œuvres Kyndryl stockés sur des supports physiquement transportés en dehors des Installations. Le Fournisseur veillera à ce qu'il soit possible de vérifier et d'établir dans quelle mesure les Œuvres Kyndryl ont été ou peuvent être transmises ou mises à disposition à l'aide d'équipements de communication de données.
- (b) **Sécurité des services réseau.** Le Fournisseur s'assurera que des contrôles et des procédures de sécurité sont mis en œuvre pour tous services et composants du réseau conformément aux pratiques normalisées de l'industrie, que ces services soient fournis en interne ou externalisés.
- (c) **Détection d'intrusions.** Le Fournisseur déploiera des systèmes de détection d'intrusions ou de prévention des intrusions et des mesures de prévention des attaques par déni de service pour tous les systèmes utilisés pour fournir les Services et les Produits et services livrables, y compris une surveillance continue pour intercepter et répondre aux événements de sécurité au fur et à mesure qu'ils sont identifiés, et mettra à jour la base de données de signatures dès que de nouvelles versions seront disponibles pour la distribution commerciale.
- (d) **Pare-feu.** Le Fournisseur mettra en place des pare-feu qui autoriseront uniquement l'utilisation des ports et services documentés et approuvés. Tous les autres ports seront en mode « refuser tout ».
- (e) **Surveillance.** Le Fournisseur surveillera l'utilisation des accès privilégiés et tiendra à jour des mesures concernant l'information sur la sécurité et gestion des événements pour : (i) identifier les accès et les activités non autorisé(e)s, (ii) faciliter une réponse rapide et appropriée à ces accès et à ces activités, et (iii) permettre des audits par le Fournisseur et Kyndryl.
- (f) **Journalisation.** Le Fournisseur doit utiliser des procédures pour garantir que tous les systèmes, y compris les pare-feu, les routeurs, les commutateurs réseau et les systèmes d'exploitation, enregistrent les informations dans leurs fonctions de journalisation système respectives ou dans un système de journalisation centralisé pour permettre les audits de sécurité mentionnés ci-dessous. Le Fournisseur doit : (i) conserver les journaux pendant au moins 180 jours, (ii) s'assurer qu'aucun journal ne contient de renseignements confidentiels, (iii) protéger les journaux contre tout(e) modification ou effacement non autorisé(e), (iv) faire une copie de sécurité des journaux au quotidien, et (v) surveiller les journaux pour détecter les risques et les anomalies fonctionnelles. Le Fournisseur fournira ces journaux à Kyndryl sur demande.

3.11. Acquisition, développement et maintenance du système

(a) Renforcement des applications

- i) Le Fournisseur tiendra à jour et mettra en place des politiques, des procédures et des normes de développement d'applications sécurisées conformément aux pratiques normalisées de l'industrie telles que le SANS Top 25 Security Development Techniques ou le projet OWASP Top Ten.
- ii) Tout le Personnel du Fournisseur responsable de la conception, du développement, de la configuration, des tests et du déploiement sécurisés d'applications sera qualifié pour exécuter les Services et les Produits et services livrables et recevra une formation appropriée concernant les pratiques de développement d'applications sécurisées du Fournisseur.

(b) Renforcement du système

- i) Le Fournisseur établira et garantira l'utilisation de configurations sécurisées standard des systèmes d'exploitation. Les images doivent représenter des versions renforcées du système d'exploitation sous-jacent et des applications installées sur le système. Le renforcement comprend la suppression des comptes inutiles (y compris les comptes de service), la désactivation ou la suppression des services inutiles, l'application de correctifs, la fermeture de ports réseau ouverts et inutilisés, et la mise en place de systèmes de détection des intrusions et/ou de systèmes de prévention des intrusions. Ces images doivent être validées régulièrement pour mettre à jour leur configuration de sécurité si nécessaire. Le Fournisseur mettra en œuvre des outils et des processus de correction pour les applications et les logiciels du système d'exploitation. Lorsque les systèmes obsolètes ne peuvent plus être corrigés, le Fournisseur effectuera une mise à jour vers la dernière version du logiciel. Le Fournisseur supprimera les logiciel obsolètes, non pris en charge et inutilisés du système.
- ii) Le Fournisseur limitera les privilèges d'administration aux seuls membres du Personnel qui ont à la fois les connaissances nécessaires pour administrer le système d'exploitation et un besoin d'affaires pour modifier la configuration du système d'exploitation sous-jacent.

(c) **Analyse de la vulnérabilité de l'infrastructure.** Le Fournisseur analysera ses environnements internes (p. ex., serveurs, appareils de réseau, etc.) liés aux Services et aux Produits et services livrables mensuellement et ses environnements externes liés aux Services et aux Produits et services livrables hebdomadairement. Le Fournisseur disposera d'un processus défini et documenté avec des délais précis pour répondre à toute constatation en fonction du risque posé et du niveau de gravité.

(d) **Évaluation de la vulnérabilité des applications.** Le Fournisseur effectuera une évaluation de la vulnérabilité de la sécurité des applications avant la publication de toute nouvelle version. Le Fournisseur disposera d'un processus défini et documenté pour répondre à toute constatation en fonction du risque posé.

(e) **Tests de pénétration et évaluations de sécurité.** Le Fournisseur fera appel à un tiers indépendant reconnu dans l'industrie pour effectuer un test de pénétration complet ainsi qu'une évaluation de sécurité de tous les systèmes impliqués dans la fourniture des Services et des Produits et services livrables, de manière récurrente, au moins une fois par an. Le Fournisseur disposera d'un processus défini et documenté pour répondre à toute constatation en fonction du risque posé. Sur demande écrite de Kyndryl, mais pas plus d'une fois par an, le Fournisseur fournira une attestation confirmant qu'un test de pénétration indépendant a été mené par un tiers et que le Fournisseur a mis en œuvre un processus pour répondre aux constatations selon une évaluation de risque. Le Fournisseur fournira un résumé des constatations, y compris le nombre de systèmes ou d'applications testés, les dates de test, la méthodologie de test et le nombre de constatations de risque critique, élevé, modéré et faible.

(f) **Reprise après sinistre.** Pendant la durée de l'Accord, le Fournisseur tiendra à jour une solution de reprise après sinistre (« DR ») ou haute disponibilité (« HA ») et un plan connexe pour les Services et les Produits et services livrables qui sont conformes aux pratiques normalisées de l'industrie. Le Fournisseur testera la solution DR ou HA et le plan connexe au moins une fois par an. De plus, la solution et le plan connexe garantiront :

- i) que les systèmes installés utilisés pour fournir les Services et les Produits et services livrables seront restaurés en cas d'interruption;
- ii) la capacité du Fournisseur à restaurer la disponibilité et l'accès aux Œuvres Kyndryl en temps opportun en cas d'incident physique ou technique, et;
- iii) la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes que le Fournisseur utilise pour fournir les Services et les Produits et services livrables.

3.12. Incidents de sécurité

- (a) Le Fournisseur tiendra à jour et suivra un programme d'intervention en cas d'incident informatique conformément aux pratiques normalisées de l'industrie, y compris des procédures documentées pour enquêter sur et intervenir en cas d'incident informatique. Le programme d'intervention en cas d'incident informatique abordera des sujets tels que la priorisation des incidents, les rôles et les responsabilités, les procédures internes d'escalade, le suivi et le signalement, ainsi que le confinement et la remédiation. Le programme de gestion des incidents de sécurité de l'information sera testé, révisé et approuvé sur une base périodique, mais au moins une fois par an.
- (b) Le Fournisseur informera rapidement (au plus tard dans les 48 heures) Kyndryl après avoir pris connaissance d'un incident de sécurité en envoyant un courriel à l'adresse cyber.incidents@kyndryl.com. En cas d'incident de sécurité, le Fournisseur devra rapidement :
- i) fournir à Kyndryl les informations raisonnablement demandées sur cet incident, l'enquête menée par le Fournisseur sur l'incident et l'état de toutes les activités de remédiation et de restauration du Fournisseur. À titre d'exemple, les informations raisonnablement demandées peuvent inclure des constatations factuelles relatives à la nature, à la cause et à l'impact de l'incident, des journaux démontrant les accès privilégiés, administratifs et autres aux appareils, aux systèmes, aux services ou aux applications, des résumés basés sur des copies judiciaires des appareils, des systèmes ou des applications, et d'autres éléments similaires, dans la mesure où cette information est pertinente à l'incident ou aux activités d'atténuation, de remédiation et de restauration du Fournisseur;
 - ii) s'assurer que le Personnel approprié du Fournisseur ayant connaissance de l'incident assiste aux conférences téléphoniques demandées par Kyndryl;
 - iii) faire appel à des experts tiers en matière d'intervention en cas d'incident informatique, de gestion des incidents d'atteinte à la protection des données, de criminalistique et de recherche électronique, à la demande raisonnable de Kyndryl;
 - iv) fournir à Kyndryl une assistance raisonnable pour satisfaire à toutes les obligations juridiques (y compris les obligations de notification aux responsables de la réglementation, aux Personnes concernées, au Client ou à d'autres tiers) de Kyndryl, des sociétés affiliées à Kyndryl et des Clients (et de leurs clients et sociétés affiliées); et
 - v) atténuer et remédier en temps opportun et de manière appropriée aux effets de l'incident de sécurité et mettre en place des contrôles et des processus supplémentaires pour réduire le risque d'incidents similaires à l'avenir, tout en tenant dûment compte de toute contribution de Kyndryl à ces atténuations et mesures correctives.
- (c) Le Fournisseur est responsable de tous les coûts et dépenses engagés par le Fournisseur pour enquêter, intervenir, atténuer et remédier à un incident de sécurité. Sous réserve de la limitation de responsabilité prévue dans l'Accord, le Fournisseur est également responsable de tous frais remboursables et dépenses engagés par Kyndryl, les sociétés affiliées à Kyndryl et les Clients (et leurs clients et sociétés affiliées) en lien avec l'enquête, l'intervention, l'atténuation et la remédiation de l'Incident de sécurité. Les coûts et les dépenses liés à la remédiation de l'Incident de sécurité peuvent inclure les coûts liés à la détection et à l'enquête sur un Incident de sécurité, la détermination des responsabilités en vertu des lois et des règlements, le rechargement des données, la correction des anomalies de produit (y compris via le code source ou autre développement), en faisant appel à des tiers pour aider avec ce qui précède ou d'autres activités pertinentes, ainsi que d'autres coûts et dépenses nécessaires pour remédier aux effets préjudiciables de l'Incident de sécurité.
- (d) En cas d'incident de sécurité impliquant les Données à caractère personnel de Kyndryl, le Fournisseur est responsable de tous les coûts qu'il engage et remboursera à Kyndryl tous les coûts et dépenses engagés par Kyndryl en rapport avec :
- i) La fourniture d'une notification de l'Incident de sécurité aux responsables de la réglementation compétents, aux autres organismes gouvernementaux et d'autorégulation du secteur d'activité concerné, aux médias (si la loi applicable l'exige), aux Personnes concernées, aux Clients et à d'autres;
 - ii) La mise en place et le maintien d'un centre d'appels pour répondre aux questions des Personnes concernées sur l'Incident de sécurité et ses conséquences, pendant 1 an après la date à laquelle ces Personnes concernées ont été informées de l'Incident de sécurité ou plus longtemps, si la loi applicable en matière de protection des données l'exige. Kyndryl et le Fournisseur travailleront ensemble pour créer les scripts et d'autres œuvres à utiliser par le personnel du centre d'appels pour répondre aux demandes de renseignements concernant les Données à caractère personnel de Kyndryl; et
 - iii) Fournir des services de protection contre l'usurpation d'identité, de surveillance du crédit et de restauration du crédit pendant deux ans à compter de la date à laquelle les personnes concernées par

- l'incident qui ont choisi de s'inscrire à ces services ont été informées de l'incident de sécurité, ou plus longtemps si la loi applicable l'exige.
- (e) Le Fournisseur n'identifiera pas, directement ou indirectement, Kyndryl auprès d'un tiers comme ayant été affectée par un Incident de sécurité, à moins que Kyndryl n'approuve cette démarche par écrit ou lorsque la loi l'exige. Le Fournisseur avisera Kyndryl par écrit avant de transmettre à un tiers toute notification exigée par la loi qui révélerait directement ou indirectement l'identité de Kyndryl.
 - (f) Le Fournisseur informera également rapidement Kyndryl de toute menace réelle ou imminente de violation des présentes Modalités ou de ses procédures de sécurité, de ses politiques de sécurité ou de ses procédures d'utilisation acceptables liées à la livraison d'un Produit ou service livrable ou aux Services.

3.13. Relations avec les fournisseurs

- (a) **Sous-traitants.** Le fournisseur est responsable du respect de ces Modalités, même s'il fait appel à un sous-traitant. Le Fournisseur obligera contractuellement ces Sous-traitants à protéger les Œuvres Kyndryl par des modalités aussi complètes et rigoureuses que celles qui s'appliquent au Fournisseur dans les Modalités. Le Fournisseur est responsable envers Kyndryl de la prestation de chaque Sous-traitant.
- (b) **Contrôle de la qualité et gestion de la sécurité.** Le Fournisseur assurera le contrôle de la qualité et de la gestion de la sécurité du développement de logiciels confié à un Sous-traitant.
- (c) **Informations précontractuelles.** Le Fournisseur déclare et garantit que toutes les informations importantes fournies au cours des discussions précontractuelles avec Kyndryl concernant la protection des renseignements personnels, la sécurité et la régie des données, que ce soit conformément aux présentes Modalités ou autrement, sont exactes dans tous leurs aspects importants et ne sont pas, par omission ou autrement, trompeuses.

3.14. Vérification, coopération, conformité en matière de sécurité et évaluation

- (a) **Vérification** Le Fournisseur conservera un registre vérifiable permettant de constater la conformité aux présentes Modalités.
 - (i) Après avoir transmis au Fournisseur un préavis écrit de trente (30) jours, Kyndryl, seul ou avec l'aide d'un auditeur externe, peut vérifier si le Fournisseur respecte les présentes Modalités, notamment en accédant à cette fin à une ou plusieurs Installations. Toutefois, Kyndryl n'accédera pas à un centre de données dans lequel le Fournisseur traite des données de Kyndryl, à moins d'avoir de bonne foi un motif de croire qu'un tel accès pourrait lui fournir de l'information pertinente. Le Fournisseur coopérera avec Kyndryl dans cette vérification, y compris en répondant intégralement et en temps opportun aux demandes d'information, que ce soit par l'entremise de documents, d'autres registres, d'entrevues avec les membres pertinents du personnel du Fournisseur ou d'autres moyens semblables. Le Fournisseur peut transmettre à Kyndryl une preuve de sa conformité à un code de conduite approuvé ou un mécanisme de certification approuvé, ou lui fournir de l'information qui peut servir à prouver qu'il respecte ces Modalités.
 - (ii) Il n'y aura pas plus d'une vérification au cours d'une période de douze (12) mois, sauf si : (a) Kyndryl doit vérifier que le Fournisseur a remédié aux problèmes constatés lors d'une vérification précédente au cours de la période de douze (12) mois; ou (b) un Incident de sécurité est survenu et Kyndryl désire vérifier le respect des obligations pertinentes à cet incident. Dans l'un ou l'autre de ces cas, Kyndryl transmettra le même avis écrit de trente (30) jours, tel que spécifié dans le paragraphe (i) plus haut. Cependant, en raison de l'urgence d'intervenir dans un cas d'Incident de sécurité, il se peut que Kyndryl soit dans l'obligation de procéder à une telle vérification dans un délai de moins de trente (30) jours suivant son avis écrit.
 - (iii) Un responsable de la réglementation ou, s'il y est légalement autorisé, tout autre Responsable du traitement peut exercer les mêmes droits que Kyndryl définis dans les paragraphes (ii) et (iii). Il est toutefois entendu qu'un responsable de la réglementation peut aussi exercer tous les droits supplémentaires que lui confère la loi.
 - (iv) Si Kyndryl a un motif raisonnable de conclure que le Fournisseur ne respecte pas l'une des présentes Modalités, que ce motif découle d'une vérification menée en vertu de ces mêmes Modalités ou autrement, le Fournisseur remédiera rapidement à cette non-conformité.
 - (v) Cette Section s'applique en plus de la clause « Tenue de registres et droit de vérification » ou à toute autre clause de vérification similaire figurant dans l'Accord.

- (b) **Coopération.** Si Kyndryl a des raisons de douter que des Services ou des Produits et services livrables aient pu contribuer, contribuent ou contribueront à un problème de cybersécurité, le Fournisseur coopérera raisonnablement à toute enquête de Kyndryl concernant ce problème, y compris en répondant intégralement et en temps opportun aux demandes d'information, que ce soit par l'entremise de documents, d'autres registres, d'entrevues avec les membres pertinents du personnel du Fournisseur, ou d'autres moyens semblables.
- (c) **Conformité en matière de sécurité.** Le Fournisseur obtiendra (i) une certification de conformité à la norme ISO 27001 de la part d'un cabinet de vérification indépendant, (ii) un rapport d'un cabinet de vérification indépendant démontrant son examen des systèmes, des contrôles et des opérations du Fournisseur conformément à une norme SOC 2 de type 2, (iii) un rapport d'un cabinet de vérification indépendant démontrant son examen des systèmes, contrôles et opérations du Fournisseur conformément à un SOC 1 de type 2, si les Services ont une incidence sur les rapports financiers de Kyndryl. Le Fournisseur se conformera aux futures directives relatives à la norme SSAE18 telles que publiées par l'AICPA, l'IAASB, la SEC ou la Public Company Accounting. Sur demande, le Fournisseur fournira rapidement à Kyndryl une copie de chaque certificat et état que le Fournisseur est tenu d'obtenir.
- (d) **Évaluation de la conformité de Kyndryl.** Sur demande raisonnable de Kyndryl, mais pas plus d'une fois par période de 12 mois pour chaque Service ou Produit ou service livrable individuel, le Fournisseur remplira avec précision et en temps opportun (dans un délai ne dépassant pas 14 jours) un questionnaire pour vérifier la conformité du Fournisseur à ses obligations en cybersécurité et de régie des données en vertu de l'Accord et des présentes Modalités (« **Évaluation de la conformité** »). Si, à l'issue de l'évaluation de la conformité, Kyndryl détermine raisonnablement que les pratiques et procédures du Fournisseur en matière de sécurité et de régie des données ne satisfont pas aux obligations du Fournisseur, Kyndryl notifiera au Fournisseur les lacunes constatées. Si le Fournisseur est d'accord avec l'évaluation des lacunes par Kyndryl, le Fournisseur devra, sans retard déraisonnable : (i) corriger ces lacunes à ses propres frais dans un délai convenu avec Kyndryl selon une évaluation du risque; et (ii) fournir à Kyndryl, ou à ses représentants dûment autorisés, une documentation et des informations raisonnables confirmant la remédiation des lacunes. Si le Fournisseur ne remédie pas aux lacunes importantes ou critiques dans les délais convenus, Kyndryl a le droit de résilier le Document de transaction applicable ou l'Accord pour manquement à une condition essentielle, immédiatement après en avoir avisé le Fournisseur. Kyndryl ne divulguera pas la documentation à aucun tiers autre que ses propres vérificateurs sans le consentement écrit du Fournisseur. Si le Fournisseur n'est pas d'accord avec l'évaluation des lacunes par Kyndryl, le Fournisseur fournira rapidement à Kyndryl une explication écrite détaillant ses raisons, et si Kyndryl n'accepte pas les raisons du Fournisseur, les parties s'adresseront à leur chef de service de protection des renseignements personnels, à leur chef de la sécurité des informations ou à un membre de la haute direction ayant un mandat et une autorité similaires afin de résoudre le différend dans les meilleurs délais. Si des anomalies sont causées par l'utilisation des Services par Kyndryl, le Fournisseur fournira une assistance technique raisonnable pour aider Kyndryl à utiliser correctement les Services afin de remédier à ces anomalies.

Article IV. ACCÈS AUX RÉSEAUX KYNDRYL

Cet article s'applique lorsque des employés du Fournisseur ont accès à un système d'entreprise.

4.1. Modalités générales

- (a) Kyndryl déterminera s'il faut ou non autoriser des employés du Fournisseur à accéder aux Systèmes d'entreprise. Si Kyndryl accorde cette autorisation, le Fournisseur devra respecter les exigences du présent Article et s'assurera que ses employés qui obtiennent un tel droit d'accès respectent également ces exigences.
- (b) Kyndryl indiquera les moyens par lesquels les employés du Fournisseur pourront accéder aux Systèmes d'entreprise, notamment si ces employés accéderont aux Systèmes d'entreprise à l'aide d'Appareils fournis par Kyndryl ou par le Fournisseur.
- (c) Les employés du Fournisseur ne peuvent accéder qu'aux Systèmes d'entreprise et ne peuvent utiliser que les Appareils que Kyndryl autorise pour cet accès, afin de fournir les Services, qui seront soit un Appareil fourni par Kyndryl (« Appareil de Kyndryl »), soit sur un Appareil fourni par le Fournisseur (« Appareil du Fournisseur »).
- (d) Les employés du Fournisseur ne copieront pas d'Œuvres de Kyndryl qui sont accessibles par l'entremise d'un Système d'entreprise, sans l'autorisation écrite préalable de Kyndryl (et ne copieront jamais de tels Œuvres dans un dispositif de stockage amovible, comme une clé USB, un disque dur externe ou un autre dispositif semblable).
- (e) À la demande de Kyndryl, le Fournisseur confirmera le nom de chacun de ses employés qui est autorisé à accéder à un Système d'entreprise, ainsi que les Systèmes d'entreprise auxquels ces employés ont accédé au cours de toute période déterminée par Kyndryl.
- (f) Le Fournisseur avisera Kyndryl dans les vingt-quatre (24) heures lorsqu'un de ses employés ayant accès à un Système d'entreprise : (a) ne fait plus partie du personnel du Fournisseur; ou (b) n'exerce plus d'activités qui nécessitent un tel accès. Le Fournisseur travaillera avec Kyndryl pour veiller à ce que le droit d'accès de ces ex-employés ou de ces employés actuels soit immédiatement révoqué.
- (g) Le Fournisseur signalera immédiatement à Kyndryl tout incident de sécurité réel ou soupçonné (comme la perte d'un Appareil de Kyndryl ou du Fournisseur, l'accès non autorisé à un Appareil de Kyndryl ou du Fournisseur ou à des Données, à des Œuvres ou à d'autres informations de toute nature) et coopérera avec Kyndryl dans l'enquête menée sur de tels incidents.
- (h) Le Fournisseur ne peut autoriser un agent, un entrepreneur indépendant ou l'employé d'un sous-traitant à accéder à un Système d'entreprise, sans obtenir le consentement écrit préalable de Kyndryl. Si Kyndryl accorde un tel consentement, le Fournisseur devra obliger contractuellement ces personnes et leur employeur à respecter les exigences du présent Article, comme si ces personnes étaient des employés du Fournisseur, et sera responsable envers Kyndryl de toutes les actions et omissions d'agir de ces personnes ou de ces employeurs en ce qui concerne l'accès à un Système d'entreprise.
- (i) Si Kyndryl croit qu'une telle mesure est nécessaire pour se protéger, elle peut révoquer en tout temps le droit d'accès aux Systèmes d'entreprise pour un ou l'ensemble des employés du Fournisseur, sans en aviser le Fournisseur, à tout employé de celui-ci ou à toute autre personne.
- (j) Les droits de Kyndryl ne sont pas entravés, affaiblis ou restreints par toute disposition du Document transactionnel, du contrat de base connexe ou de tout autre accord conclu entre les parties, y compris toute disposition pouvant exiger de conserver des Données, des Œuvres ou d'autres informations de quelque nature que ce soit à un ou plusieurs endroits définis, ou que seules des personnes situées à un ou plusieurs endroits définis aient accès à de telles Données, Œuvres ou autres informations.

4.2. Logiciels des Appareils

- (a) Le Fournisseur demandera à son personnel d'installer en temps opportun les logiciels sur les Appareils de Kyndryl et les Appareils du Fournisseur dont Kyndryl a besoin pour permettre l'accès aux Systèmes d'entreprise de manière sécurisée. Le Fournisseur et son Personnel ne sont pas autorisés à entraver le fonctionnement de ces logiciels ou des fonctions de sécurité activées par ces logiciels.
- (b) Le Fournisseur et son Personnel adhéreront aux règles configuration des Appareils de Kyndryl et des Appareils du Fournisseur définies par Kyndryl et travailleront par ailleurs avec Kyndryl pour garantir que les logiciels fonctionnent comme Kyndryl le souhaite. Par exemple, le Fournisseur ne contournera pas les fonctions de blocage de sites Web ou d'application automatique de correctifs des logiciels.
- (c) Le Personnel du Fournisseur ne peut pas partager les noms d'utilisateur, les mots de passe ou autres éléments similaires des Appareils de Kyndryl et des Appareils du Fournisseur avec toute autre personne.
- (d) Si Kyndryl autorise le Personnel du Fournisseur à accéder à des Systèmes d'entreprise à l'aide d'Appareils du Fournisseur, ce dernier devra installer et exécuter sur ces Appareils un système d'exploitation approuvé par Kyndryl, mais aussi effectuer une mise à niveau vers une nouvelle version de ce système d'exploitation ou vers un nouveau système d'exploitation dans un délai raisonnable après avoir reçu de telles instructions de la part de Kyndryl.

4.3. Appareils de Kyndryl

- (a) Les employés du Fournisseur ne sont pas autorisés à se servir des Appareils de Kyndryl pour fournir des Services à toute autre personne ou entité, ni pour accéder à des systèmes informatiques, à des réseaux, à des applications, à des sites Web, à des outils de courriel ou de collaboration ou à des éléments semblables du Fournisseur ou d'un tiers pour les Services ou en lien avec ceux-ci. Les employés du Fournisseur ne peuvent pas utiliser les Appareils de Kyndryl pour des raisons personnelles (p. ex., les employés du Fournisseur ne peuvent pas sauvegarder de fichiers personnels tels que de la musique, des vidéos, des images ou d'autres éléments similaires sur ces Appareils de Kyndryl et ne peuvent pas utiliser Internet à partir de ces Appareils de Kyndryl pour des raisons personnelles). Les employés du Fournisseur ne peuvent pas partager les Appareils de Kyndryl qu'ils utilisent pour accéder aux Systèmes d'entreprise avec d'autres employés du Fournisseur.
- (b) Kyndryl a le droit absolu de surveiller les Appareils de Kyndryl et les Systèmes d'entreprise et de remédier à une intrusion potentielle et à d'autres menaces de cybersécurité de quelque manière que ce soit, à partir de n'importe quel endroit et en utilisant les moyens que Kyndryl juge nécessaires ou appropriés, sans fournir de préavis au Fournisseur, aux employés de celui-ci ou à toute autre personne. À titre d'exemple, Kyndryl peut en tout temps : (i) effectuer un test de sécurité sur tout Appareil de Kyndryl; (ii) surveiller, récupérer par des moyens techniques ou autres et passer en revue les communications (dont les courriels issus de tout compte de courriel sur les Appareils de Kyndryl), des enregistrements, des fichiers et d'autres éléments enregistrés dans tout Appareil de Kyndryl ou transmis par l'entremise d'un Système d'entreprise; et (iii) acquérir une copie juridique intégrale de tout Appareil de Kyndryl. Si Kyndryl nécessite la coopération du Fournisseur pour exercer ses droits, le Fournisseur répondra intégralement et en temps opportun aux demandes de Kyndryl pour une telle coopération. Il peut s'agir, par exemple, de demandes pour configurer tout Appareil de Kyndryl, d'installer des logiciels de surveillance ou un autre type de logiciel dans un Appareil de Kyndryl, de partager des détails sur les connexions à un système, de participer aux mesures d'intervention en cas d'incident avec un Appareil et de fournir un accès physique à tout Appareil de Kyndryl pour permettre à Kyndryl d'obtenir une copie judiciaire intégrale ou d'autres demandes semblables et connexes.
- (c) Kyndryl conservera la propriété de tous ses Appareils de Kyndryl, alors que le Fournisseur assumera le risque de perte de ces Appareils de Kyndryl, y compris en raison d'un vol, de vandalisme ou de négligence. Le Fournisseur ne modifiera pas ou ne permettra pas de modifier les Appareils de Kyndryl sans obtenir au préalable le consentement écrit de Kyndryl. La modification d'un appareil comprend notamment toute modification apportée aux logiciels, aux applications, à la conception et à la configuration de la sécurité de l'Appareil ou à sa conception physique, mécanique ou électrique.
- (d) Le Fournisseur retournera tous les Appareils de Kyndryl dans les cinq (5) jours ouvrables à compter du moment où ces Appareils ne sont plus nécessaires pour fournir les Services. Il devra aussi, si Kyndryl le demande, détruire simultanément dans ces Appareils l'ensemble des Données, des Œuvres et d'autres informations de quelque nature que ce soit, sans en conserver une copie, en suivant les normes du NIST, afin d'effacer de manière permanente toutes ces Données, ces Œuvres et autres informations. Le Fournisseur emballera et retournera à ses propres frais les Appareils de Kyndryl à l'endroit indiqué par Kyndryl, et ce, dans la même condition qu'ils étaient au moment de leur livraison au Fournisseur, exception faite de l'usure raisonnable. Tout manquement du Fournisseur à l'une ou l'autre des obligations définies dans le présent paragraphe (d) constituera un manquement à une conditions essentielle du Document transactionnel, du contrat de base connexe et de tout autre accord afférent conclu entre les parties. Un accord est considéré comme étant « afférent » si l'accès à un Système d'entreprise facilite les tâches ou d'autres activités du Fournisseur aux termes de ce même accord.
- (e) Kyndryl fournira de l'assistance pour ses Appareils et procédera notamment à leur inspection et à leur maintenance préventive et corrective. Le Fournisseur doit aviser promptement Kyndryl de tout besoin de maintenance corrective.
- (f) Pour les logiciels dont Kyndryl est propriétaire ou a le droit d'accorder une licence, Kyndryl accorde au Fournisseur un droit temporaire d'utiliser, de stocker et de faire suffisamment de copies pour permettre son utilisation autorisée des Appareils de Kyndryl. Il est interdit au Fournisseur de transférer les logiciels à quiconque, de faire des copies de l'information sur la licence des logiciels ou de désassembler, de décompiler, de rétroconcevoir ou de convertir autrement les logiciels, à moins que cela ne soit expressément permis par les lois applicables, sans possibilité de renonciation contractuelle.

Article V. DÉFINITIONS

Les termes « Services » et « Produits et services livrables » sont probablement définis dans le Contrat de relation Fournisseur, un contrat équivalent ou un Document transactionnel. Sinon, le terme « **Services** » désigne tout Service hébergé, services-conseils, d'installation, de personnalisation, de maintenance, d'assistance, de personnel d'appoint, d'affaires, techniques ou d'autres travaux que le Fournisseur effectue pour Kyndryl, tel que spécifié dans le Document transactionnel. Le terme « **Produits et services livrables** » désigne pour sa part tout logiciel, plateforme, application ou d'autres produits ou éléments et leurs Œuvres respectives que le Fournisseur fournit à Kyndryl, tel que spécifié dans le Document transactionnel.

- 5.1. **Pays adéquat** Pays offrant un niveau adéquat de protection des Données en ce qui concerne le transfert en question, conformément aux lois applicables en matière de protection des Données ou aux décisions des organismes de réglementation.
- 5.2. **Système d'IA** désigne un système automatisé conçu pour fonctionner avec différents niveaux d'autonomie, qui peut s'adapter après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des intrants qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.
- 5.3. **Coordonnées professionnelles** (« **BCI** ») désigne les Données à caractère professionnel utilisées pour communiquer, identifier ou authentifier une personne dans un rôle professionnel ou commercial à des fins administratives et de gestion des contrats (p. ex., la facturation et la gestion des comptes, le calcul des mesures incitatives des partenaires, la présentation de l'information financière à l'interne et la modélisation commerciale telles que les prévisions, les revenus et la planification de la capacité). Le plus souvent, les Coordonnées professionnelles incluent le nom d'une personne, de même que son adresse de courriel, son adresse physique, son numéro de téléphone au travail ou des renseignements semblables. Par exemple, les noms et les adresses de courriel utilisés pour contacter le Personnel du Fournisseur pour des services de soutien sont des Coordonnées professionnelles; cependant, les noms et les adresses de courriel inclus dans les données d'assistance diagnostique sont des Données à caractère personnel de Kyndryl.
- 5.4. **Service infonuagique** désigne toute offre « à la demande » que le Fournisseur héberge ou gère, dont un « logiciel à la demande », une « plateforme à la demande » et une « infrastructure à la demande ».
- 5.5. **Responsable du traitement** désigne toute personne physique ou morale, autorité publique, organisme ou tout autre entité qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de Données à caractère personnel.
- 5.6. **Système d'entreprise** désigne un système informatique, une plateforme, une application, un réseau ou un élément semblable sur lesquels s'appuie Kyndryl pour mener ses activités d'entreprise, y compris ceux qui se trouvent sur ou qui sont accessibles via l'intranet de Kyndryl, l'Internet ou autrement.
- 5.7. **Client** désigne un Client de Kyndryl.
- 5.8. **Importateur de données** désigne un sous-traitant ou un sous-traitant ultérieur qui n'est pas établi dans un Pays adéquat.
- 5.9. **Personne concernée** désigne une personne physique qui peut être identifiée, directement ou indirectement.
- 5.10. **Jour** ou **Jours** désigne un (des) jour(s) civil(s), à moins que jour ne soit immédiatement suivi du mot « ouvrable », auquel cas il s'agit d'un jour ouvrable.
- 5.11. **Appareil** désigne un poste de travail, un ordinateur portable, une tablette, un téléphone intelligent ou un assistant numérique personnel fourni par Kyndryl ou le Fournisseur.
- 5.12. **Installations** désigne un lieu physique où le Fournisseur héberge, accède ou traite autrement des Produits et services livrables ou des Œuvres de Kyndryl.
- 5.13. **Pratiques normalisées de l'industrie** désigne les pratiques qui respectent celles qui sont recommandées ou exigées par le National Institute of Standards and Technology (« **NIST** ») ou l'Organisation internationale de normalisation (« **ISO** »), ou tout autre organisme ou organisation jouissant d'une réputation et présentant un savoir-faire semblables.
- 5.14. **Données de Kyndryl** désigne toutes les données, les fichiers, les œuvres, les textes, les enregistrements audio, les vidéos, les images ou autres données, y compris les Données à caractère personnel de Kyndryl, les Coordonnées professionnelles (BCI) de Kyndryl et les Données à caractère non personnel de Kyndryl, qui sont fournies au Fournisseur ou accessibles par celui-ci (y compris, sans limitation, via un service infonuagique) en lien avec la fourniture des Services ou des Produits et services livrables, qu'ils soient fournis ou rendus accessibles par Kyndryl, le Personnel de Kyndryl, un Client, un employé ou un sous-traitant d'un Client, ou toute autre personne ou entité.
- 5.15. **Œuvres Kyndryl** désigne toute donnée de Kyndryl et technologie de Kyndryl.

- 5.16. **Données à caractère personnel de Kyndryl** désigne les Données à caractère personnel, à l'exclusion des Coordonnées professionnelles de Kyndryl, que Kyndryl fournit ou rend accessibles au Fournisseur pour la fourniture des Services ou des Produits et services livrables. Les Données à caractère personnel de Kyndryl comprennent les Données à caractère personnel que Kyndryl gère et traite au nom d'autres Responsables du traitement.
- 5.17. **Technologie Kyndryl** désigne le code source, les autres codes, les langages de description, les micrologiciels, les logiciels, les outils, les conceptions, les schémas, les représentations graphiques, les clés intégrées, les certificats et autres informations, les Œuvres, les biens, les documents et les technologies que Kyndryl a directement ou indirectement accordé sous licence au Fournisseur ou mis autrement à sa disposition en lien avec le Document transactionnel ou l'Accord.
- 5.18. **Pays non adéquat** désigne un pays qui n'est pas considéré comme adéquat en vertu des lois applicables en matière de protection des données ou d'une décision d'un responsable de la réglementation compétent.
- 5.19. **Autre responsable du traitement** désigne toute entité autre que Kyndryl qui agit en tant que Responsable du traitement des Données de Kyndryl, comme une société affiliée de Kyndryl, un Client ou la société affiliée d'un Client.
- 5.20. **Logiciels sur site** désigne les logiciels fournis par le Fournisseur en tant que Produit ou service livrable que Kyndryl ou un sous-traitant de Kyndryl exécute, installe ou exploite sur les serveurs ou systèmes de Kyndryl ou du sous-traitant.
- 5.21. **Données à caractère personnel** désigne toute information relative à une Personne concernée et toute autre information qualifiée de « Données à caractère personnel » ou équivalent en vertu de toute loi sur la protection des données.
- 5.22. **Personnel** désigne les personnes qui sont des employé(e)s ou des agents de Kyndryl ou du Fournisseur, des sous-traitants indépendants engagés par Kyndryl ou le Fournisseur, ou mis à disposition d'une partie par un sous-traitant.
- 5.23. **Traiter** ou **traitement** désigne toute opération ou ensemble d'opérations exécutées sur les Données de Kyndryl, y compris le stockage, l'utilisation, l'accès et la lecture.
- 5.24. **Sous-traitant** désigne une personne physique ou morale qui traite des Données à caractère personnel au nom d'un Responsable du traitement et inclut « fournisseur de services » ou des termes essentiellement semblables en vertu de toute loi sur la protection des données.
- 5.25. **Incident de sécurité** désigne (a) une situation qui met en péril de manière réelle ou imminente la confidentialité, l'intégrité ou la disponibilité de toute Œuvre de Kyndryl ou d'un système d'information utilisé par le Fournisseur ou par ses Sous-traitants pour fournir les Services ou les Produits et services livrables, (b) une violation de sécurité entraînant la destruction accidentelle ou illicite, la perte, la modification, la divulgation ou l'accès non autorisé aux Données de Kyndryl transmises, stockées ou autrement traitées, ou (c) l'accès non autorisé ou l'utilisation du code source utilisé par le Fournisseur ou ses Sous-traitants dans le cadre de la fourniture des Services ou des Produits et services livrables ou en rapport avec ceux-ci.
- 5.26. **Vendre** (ou **Vente**) signifie louer, libérer, divulguer, diffuser, mettre à disposition, transférer ou communiquer de toute autre manière, oralement, par écrit, par voie électronique ou par d'autres moyens, des Données en échange d'une contrepartie monétaire ou d'une autre valeur.
- 5.27. **Partager** a la signification qui lui est donnée dans le California Consumer Privacy Act de 2018, tel que modifié par le Consumer Privacy Rights Act de 2020.
- 5.28. **Clauses contractuelles types** (« CCT ») désigne les clauses contractuelles requises par les lois sur la protection des Données applicables pour le transfert de Données à caractère personnel à des Responsables du traitement ou des Sous-traitants qui ne sont pas établis dans un Pays adéquat.
- 5.29. **Code source** désigne un code de programmation lisible par l'humain ou un code susceptible d'être converti en un format lisible par l'humain que les développeurs utilisent pour créer, développer ou mettre à jour un produit, mais qui n'est pas rendu public dans le cadre normal de la distribution commerciale ou l'utilisation du produit.
- 5.30. **Sous-traitant ultérieur** désigne tout sous-traitant du Fournisseur, incluant une société affiliée du Fournisseur, qui traite des Données à caractère personnel de Kyndryl.
- 5.31. **Autorité de contrôle** désigne un organisme public indépendant chargé de superviser l'application des lois sur la protection des données dans un pays ou une région spécifique.