

CONDITIONS DE CONFIDENTIALITÉ ET DE SÉCURITÉ DU FOURNISSEUR

Les présentes Conditions de confidentialité et de sécurité définissent les droits et obligations de Kyndryl et du Fournisseur concernant la gouvernance des données, la sécurité et les sujets connexes (les « **Conditions** »). Les Conditions sont intégrées et font partie de l'Accord de Relation Fournisseur (ou accord équivalent) entre les parties, y compris les Déclarations de Travail, les Autorisations de Travail, ou d'autres éléments entre nos entreprises qui y font référence (les « **Éléments transactionnels** »).

Les présentes Conditions comprennent :

- Le présent document,
- L'Annexe relative aux détails du traitement jointe au présent document décrit les activités de traitement des données effectuées par le Fournisseur à compter de l'exécution des présentes conditions (pour tout Document de Transaction conclu après l'exécution des présentes conditions, une Annexe relative aux détails du traitement distincte sera jointe à chaque Document de Transaction, afin de documenter les activités de traitement effectuées par le Fournisseur spécifiques à ce document), et
- les clauses contractuelles types de l'UE, l'addendum britannique sur le transfert international de données et l'évaluation de l'impact du transfert par le fournisseur se trouvent à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.

En cas de conflit entre les dispositions des présentes Conditions, du Contrat de Relation fournisseur, d'un accord équivalent ou d'un Document de Transaction, y compris de tout accord de traitement des données, les présentes Conditions prévaudront. En cas de conflit entre les présentes Conditions et les dispositions mutuellement convenues entre le Fournisseur et Kyndryl pour un client de Kyndryl, les dispositions mutuellement convenues pour un client de Kyndryl prévaudront.

Les termes en majuscules ont les significations données à l'Article V des présentes Conditions, ou ailleurs dans ces Conditions, ou dans le Document de Transaction ou l'accord de base associé entre les parties.

Article I. GOUVERNANCE DES DONNÉES ET IA

- 1.1. **Respect des lois.** Le Fournisseur respectera toutes les lois applicables aux Services et aux Livrables, y compris les lois relatives à la protection des données, à la cyber-sécurité et aux systèmes d'IA. Le Fournisseur avertira Kyndryl rapidement (et en tout état de cause dans les délais requis par la loi et donnant à Kyndryl la possibilité de s'acquitter de ses propres obligations légales) s'il détermine qu'il ne peut plus remplir ses obligations légales.
- 1.2. **Utilisation des données.** Le Fournisseur ne doit pas :
 - (a) utiliser les données de Kyndryl sous quelque forme que ce soit, y compris agrégées, anonymisées ou autrement, à des fins autres que la fourniture des Services et des Livrables (à titre d'exemple, le Fournisseur n'est pas autorisé à utiliser ou réutiliser les Données de Kyndryl pour évaluer l'efficacité ou les moyens d'améliorer ses offres autres que les Services ou les Livrables, pour la recherche et le développement, afin de créer de nouvelles offres, ou pour générer des rapports concernant les offres du Fournisseur)
 - (b) vendre ou partager les Données de Kyndryl ou
 - (c) tenter de réidentifier toute information qui peut raisonnablement être utilisée pour déduire des informations sur une personne concernée ou être liée à celle-ci de quelque manière que ce soit.
- 1.3. **Technologies de suivi Web.** Si le Fournisseur ou ses Sous-traitants, dans le cadre de la fourniture des Services ou des Livrables, collectent des données à l'aide de technologies de suivi Web (y compris HTML5, stockage local, balises ou jetons de tiers et balises Web), ces données sont considérées comme des Données de Kyndryl et le Fournisseur se conformera à ses obligations concernant les Données Kyndryl en vertu des présentes Conditions.
- 1.4. **Non-divulgaration.** Le Fournisseur ne divulguera pas les Données de Kyndryl à un tiers autre que les Sous-traitants des données approuvés conformément à la section 2.5 ou les Sous-traitants approuvés conformément à l'Accord.
- 1.5. **Accès du gouvernement.** Si un gouvernement, y compris tout organisme de régulation, exige l'accès aux données de Kyndryl (par exemple, si le gouvernement américain délivre un ordre relatif à la sécurité nationale

au Fournisseur pour obtenir les données de Kyndryl), ou qu'une divulgation des données de Kyndryl est exigée par la loi, le Fournisseur notifiera rapidement Kyndryl par écrit de cette demande ou de cette exigence et donnera à Kyndryl une possibilité raisonnable de contester toute divulgation, sauf si la loi l'interdit. Si la notification est interdite par la loi, le Fournisseur prendra les mesures qu'il estime raisonnablement appropriées pour contester l'interdiction et la divulgation des Données de Kyndryl par le biais d'une action en justice ou par d'autres moyens.

- 1.6. **Confidentialité.** Le Fournisseur garantit à Kyndryl que : (a) seuls les membres de son personnel qui ont besoin d'accéder aux Données de Kyndryl pour fournir les Services ou Livrables obtiendront cet accès et uniquement dans les limites nécessaires ; et (b) qu'il a soumis ses employés à des obligations de confidentialité exigeant que ses employés utilisent et divulguent les Données de Kyndryl uniquement dans les limites autorisées par les présentes Conditions.
- 1.7. **Restitution ou suppression des Données de Kyndryl.** Le Fournisseur supprimera ou restituera, à la discrétion de Kyndryl, les Données de Kyndryl à ses propres frais, à la résiliation ou l'expiration du Document de Transaction, ou à une date antérieure sur demande de Kyndryl. Si Kyndryl demande la suppression, le Fournisseur s'engage, conformément à la norme NIST SP 800-88 rév.1, à rendre les données illisibles et impossibles à réassembler ou à reconstituer et certifiera à Kyndryl la suppression. Si Kyndryl exige le retour des Données de Kyndryl, le Fournisseur le fera dans un format couramment utilisé, selon le calendrier et les instructions raisonnables de Kyndryl.
- 1.8. **Systèmes d'IA**
 - (a) Le Fournisseur ne doit pas utiliser des systèmes d'IA dans la fourniture des Services ou d'un Livrable, ni inclure des systèmes d'IA dans un Livrable, sans autorisation préalable de Kyndryl dans un Document de Transaction ou dans l'Accord. En sollicitant l'autorisation de Kyndryl, le Fournisseur fournira par écrit à Kyndryl toutes les informations nécessaires pour évaluer l'utilisation des systèmes d'IA par le Fournisseur (par exemple, les flux de données, les modèles de langage utilisés, la séparation des données).
 - (b) Le Fournisseur déclare et garantit que : (i) les entrées fournies par Kyndryl (y compris les entrées fournies par les employés ou toute autre tierce partie en vertu d'un Document de Transaction), et que les résultats générés seront classifiés comme des Éléments de Kyndryl, (ii) que le Fournisseur n'utilisera pas les Éléments de Kyndryl pour entraîner ou affiner le modèle de base ou d'autres éléments des Systèmes d'IA, (iii) que le Fournisseur ne stockera pas les Éléments de Kyndryl plus longtemps que nécessaire pour fournir les Services, (iv) que les Systèmes d'IA (y compris les résultats générés et les données d'entraînement seront classifiés comme faisant partie des Services, et (v) dans la mesure permise par la loi applicable, que le Fournisseur cède à Kyndryl par la présente l'ensemble de ses droits, titres et intérêts dans et sur les résultats générés par les Systèmes d'IA.
 - (c) Le Fournisseur met en œuvre et maintient un programme documenté de gouvernance et de gestion des risques pour les systèmes d'IA, qui identifie, teste, surveille et atténue 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 ces derniers. Sur demande, le Fournisseur partagera une copie de son programme de gouvernance et de gestion des risques pour les systèmes d'IA. Le Fournisseur avisera rapidement Kyndryl par écrit de tout risque survenu ou de tout risque matériel identifié conformément à la disposition de notification convenue dans le Document de transaction en envoyant une copie à ailegalteam@kyndryl.com.

Article II. CONFIDENTIALITÉ

- 2.1. **Coordonnées des Contacts Professionnels.** Kyndryl et le Fournisseur peuvent traiter les Coordonnées professionnelles de l'autre partie conformément aux lois applicables en matière de protection des données en tant que Responsables indépendants du traitement partout où ils exercent leurs activités, afin de distribuer et de recevoir les Livrables et les Services. Les parties ne jouent pas le rôle de Responsables conjoints du traitement concernant les Coordonnées professionnelles de l'autre partie. Si l'une des parties informe l'autre partie de toute demande d'une personne concernée relative aux Coordonnées professionnelles de l'autre partie, cette dernière sera chargée de traiter ces demandes directement avec la personne concernée. Chacune des parties a mis en œuvre des mesures techniques et organisationnelles appropriées pour protéger les Coordonnées professionnelles de l'autre partie. Dans un souci de clarté, la Section 3.12 (Incidents de sécurité) s'applique aux Coordonnées professionnelles.

- 2.2. Fournisseur comme Processeur des données.** Kyndryl désigne le Fournisseur comme Processeur des données à caractère personnel Kyndryl dans le seul but de fournir les Livrables et les Services conformément aux instructions de Kyndryl, y compris celles contenues dans les présentes Conditions, l'Accord et tout Document de Transaction connexe. Le Fournisseur est un Processeur de données à caractère personnel de Kyndryl. Si le Fournisseur n'agit pas conformément aux instructions de Kyndryl, afin que Kyndryl se conforme à la législation applicable en matière de protection des données, Kyndryl peut mettre fin à la partie concernée des Services par notification écrite. Si le Fournisseur estime qu'une instruction enfreint une loi sur la protection des données, le Fournisseur s'engage à en informer Kyndryl rapidement et dans les délais requis par la loi.
- 2.3. Mesures techniques et organisationnelles.** Le Fournisseur mettra en œuvre et maintiendra des mesures techniques et organisationnelles appropriées, y compris les mesures de sécurité mentionnées à l'article III ci-dessous, pour garantir un niveau de sécurité adapté au risque associé à la fourniture des Services et Livrables.
- 2.4. Droits et Demandes des Personnes Concernées**
- (a) Le Fournisseur s'engage à informer Kyndryl rapidement (dans un délai permettant à Kyndryl et aux autres Responsables de traitement de respecter leurs obligations légales) de toute demande émanant d'une Personne concernée en vue d'exercer ses droits (tels que son droit de rectification, de suppression ou de blocage de données) concernant les Données à caractère personnel de Kyndryl. Le Fournisseur pourra également orienter rapidement une Personne concernée faisant une telle demande vers Kyndryl. Le Fournisseur ne répondra pas aux demandes émanant des Personnes concernées, sauf en vertu d'une obligation légale ou sur instruction écrite de Kyndryl.
 - (b) Si Kyndryl est tenue de fournir des informations relatives aux Données à caractère personnel de Kyndryl à d'autres Responsables de traitement ou à des tiers (par exemple, les Personnes concernées ou les autorités compétentes), le Fournisseur assistera Kyndryl en fournissant les informations et en prenant d'autres mesures raisonnables demandées par Kyndryl, selon un calendrier permettant à Kyndryl de répondre dans les délais auxdits Responsables du traitement ou tiers.
- 2.5. Sous-traitants ultérieurs**
- (a) Kyndryl autorise le Fournisseur à engager les Sous-traitants des données répertoriés dans les Annexes correspondantes relatives aux détails du traitement. Le Fournisseur peut également recourir à des Sous-traitants des données supplémentaires ou de remplacement, ou élargir le champ de Traitement par un Sous-traitant des données existant, sous réserve des conditions suivantes :
 - (i) Le Fournisseur fournira à Kyndryl un préavis écrit avant de procéder à toute modification de ce type.
 - (ii) Kyndryl pourra s'opposer à tout nouveau Sous-traitant des données, à tout remplacement de Sous-traitant des données ou à toute extension du champ du traitement pour des motifs raisonnables, et les parties travailleront ensemble de bonne foi pour répondre à l'objection de Kyndryl.
 - (iii) Sans préjudice du droit de Kyndryl de s'y opposer à tout moment, le Fournisseur peut procéder à la modification si Kyndryl n'a pas émis d'objection dans un délai de 30 jours après réception du préavis écrit du Fournisseur.
 - (b) Le Fournisseur imposera les obligations de protection des données, de sécurité et de certification énoncées dans les présentes Conditions à chaque Sous-traitant des données approuvé, avant qu'un Sous-traitant des données traite des Données à caractère personnel de Kyndryl. Le Fournisseur demeure entièrement responsable vis-à-vis de Kyndryl du respect des obligations de chaque Sous-traitant des données.
- 2.6. Traitement de données transfrontalier**
- (a) Le Fournisseur ne transférera ni ne divulguera (y compris par accès distant) aucune Donnée à caractère personnel de Kyndryl au-delà des frontières, sauf aux Sous-traitants des données approuvés conformément à la Section 2.5. Si Kyndryl approuve le transfert transfrontalier des Données à caractère personnel de Kyndryl, les parties coopéreront pour respecter les lois applicables de protection des données. Si des Clauses Contractuelles Types (CCT) sont exigées par ces lois, le Fournisseur conclura rapidement les CCT telles que définies ci-dessous.
 - (b) **Espace économique européen**
 - (i) Si Kyndryl transfère des Données Personnelles 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 accepte par la présente de conclure les Clauses Contractuelles Types de l'UE (Décision de la Commission 2021/914), pré-signées par Kyndryl et disponibles à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms> (« CCT de l'UE »).
- (ii) En cas de disparition effective de Kyndryl, de cessation de son existence en loi, ou de son insolvabilité, les Autres Responsables du traitement auront le droit de mettre fin à l'Accord et d'inviter le Fournisseur à effacer ou retourner les Données Personnelles de Kyndryl.
 - (iii) L'évaluation de Kyndryl concernant les transferts de Données Personnelles aux Fournisseurs, telle que requise par les Clauses CCT de l'UE, est publiée pour examen par le Fournisseur à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
 - (iv) Le Fournisseur fournira des détails suffisants sur chaque Sous-traitant des données dans les Annexes des Détails de Traitement et dans les notifications, afin de 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 des données, les lieux de traitement et les activités de traitement.
 - (v) Le Fournisseur agira en tant qu'Exportateur de données et acceptera les clauses CCT de l'UE ou tout autre mécanisme de transfert approprié avec chaque Sous-traitant des données approuvé non établi dans un pays adéquat.
- (c) **Royaume-Uni.** Si des Données à caractère personnel de Kyndryl soumises à la loi britannique de 2018 sur la protection des données (UK Data Protection Act 2018) sont transférées en dehors du Royaume-Uni vers un Pays non adéquat, le Fournisseur accepte par la présente l'addendum britannique sur le transfert international de données (UK International Data Transfer Addendum) préalablement signé par Kyndryl et disponible à l'adresse <https://www.kyndryl.com/procurement/terms/privacy-and-security-terms>.
- (d) **Suisse.** Si des Données Personnelles de Kyndryl soumises à la Loi fédérale suisse sur la protection des données (« LPD ») sont transférées en dehors de la Suisse vers un Pays Non Adéquat, le Fournisseur accepte par la présente les Clauses Contractuelles Types (CCT) de l'UE, sous réserve des modifications suivantes :
- (i) la référence au RGPD doit également inclure la référence aux dispositions équivalentes de la LPD ;
 - (ii) la Commission fédérale suisse de protection des données est l'autorité de surveillance exclusive conformément à la clause 13 et à l'Annexe I.C des clauses CCT de l'UE ;
 - (iii) la loi applicable conformément à la clause 17 des clauses CCT de l'UE sera la loi suisse si le transfert de données est exclusivement soumis à la LPD ; et
 - (iv) le terme « état membre » ne doit pas être interprété de manière à exclure les personnes concernées en Suisse de la possibilité d'exercer leurs droits dans leur lieu de résidence habituelle (Suisse), conformément à l'article 18 des CCT de l'UE.
- (e) **Brésil.** Si Kyndryl transfère des Données à caractère personnel soumises à la Lei Geral de Proteção de Dados (LGPD) en dehors du Brésil à un Fournisseur non établi dans un Pays adéquat, le Fournisseur accepte par la présente l'Annexe II de la Resolução CD/ANPD n° 19/2024 (ci-après dénommée « 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 dans lequel soit les clauses CCT locales n'ont pas été publiées par l'autorité de contrôle (par exemple, la Loi péruvienne sur la protection des données, la Loi sud-africaine sur la protection des données), soit l'autorité de contrôle a approuvé l'utilisation de clauses contractuelles types (CCT) de l'UE comme garantie suffisante pour le transfert transfrontalier (par exemple, la Loi argentine sur la protection des données), les clauses CCT de l'UE régiront ledit transfert sous réserve des modifications suivantes :
- (i) les références au RGPD doivent également inclure la référence aux dispositions équivalentes de la loi locale sur la protection des données ;
 - (ii) l'autorité de supervision locale est l'autorité de supervision exclusive, conformément à la Clause 13 et à l'Annexe I.C des clauses CCT de l'UE ;
 - (iii) La loi applicable conformément à la clause 17 des clauses CCT 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 d'exercer leurs droits dans leur lieu de résidence habituelle, conformément à l'article 18 des clauses CCT de l'UE.

2.7. Assistance et enregistrements

- (a) Compte tenu de la nature du Traitement, le Fournisseur aidera Kyndryl en prenant des mesures techniques et organisationnelles appropriées (« MTO ») pour remplir les obligations associées aux demandes et aux droits

de la Personne concernée. Le Fournisseur assistera également Kyndryl pour s'assurer de la conformité aux obligations relatives à la sécurité du Traitement, à la notification et à la communication d'un Incident de Sécurité et la création d'évaluations d'impact sur la protection des données, notamment la consultation préalable de l'autorité compétente, si nécessaire, en prenant en considération les informations à la disposition du Fournisseur.

- (b) Le Fournisseur s'engage à conserver un registre à jour du nom et des coordonnées de chaque Sous-traitant des données, notamment de chaque représentant de et délégué à la protection des données de chaque Sous-traitant des données. Sur demande, le Fournisseur transmettra ce registre à Kyndryl dans un délai permettant à Kyndryl de répondre rapidement à toute demande émanant d'un Client ou d'un tiers.

2.8. Dispositions nationales spécifiques

(a) Japon

- i) Pour les Coordonnées professionnelles des personnes concernées situées au Japon, le Fournisseur respectera les dispositions des présentes conditions, applicables au Fournisseur en tant que Processeur de données.
- ii) La définition d'« Incident de Sécurité » dans les présentes Conditions est modifiée par la présente pour inclure les violations raisonnablement suspectées des Données Personnelles de Kyndryl concernant les Personnes concernées situées au Japon.
- iii) Le Fournisseur garantit qu'il n'a aucun motif de croire que les lois et pratiques de tout pays où le Fournisseur ou ses Sous-traitants des données traiteront les Données à caractère personnel de Kyndryl l'empêchent de remplir ses obligations en vertu de ces Conditions. Le Fournisseur informera Kyndryl si, après avoir accepté les conditions et pendant la durée de celles-ci, il a des raisons de croire qu'il ne peut pas se conformer à ses obligations en vertu des Conditions. 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 déterminera 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 des personnes concernées situées dans l'État de Californie, (i) Kyndryl ne divulgue les Données à caractère personnel de Kyndryl au Fournisseur qu'aux fins commerciales limitées et spécifiées sélectionnées dans l'Annexe applicable des détails du traitement, (ii) Kyndryl peut, sur notification, 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 pas, n'utilisera pas ou ne divulguera pas les Données personnelles de Kyndryl en dehors de la relation d'affaires directe entre Kyndryl et le Fournisseur.

(c) Canada.

- i) Pour les Coordonnées professionnelles des personnes concernées situées au Canada, le Fournisseur respectera les dispositions des présentes Conditions, applicables au Fournisseur en tant que Processeur de données, dans la mesure où elles sont considérées comme des Données à caractère personnel.
- ii) Pour plus de clarté, les références aux lois applicables en matière de protection des données incluent, sans limitation, toutes les lignes directrices 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 de mesures à des fins d'identification personnelle.
- iv) Le Fournisseur effectuera toute évaluation d'impact sur la confidentialité ou d'impact sur le transfert requise en vertu des lois sur la protection des données en vigueur au Canada, fournira un exemplaire de ces évaluations sur demande et informera Kyndryl, sans retard injustifié, de toute mesure supplémentaire à appliquer.
- v) Dans le cas où Kyndryl ne serait pas d'accord avec les résultats des évaluations du Fournisseur ou les mesures supplémentaires, Kyndryl et le Fournisseur travailleront ensemble pour trouver une solution réalisable. Dans l'hypothèse où les Parties ne parviendraient pas à s'accorder sur une solution réalisable, Kyndryl se réserve le droit de suspendre ou de résilier les services concernés du Fournisseur, sans indemnisation.
- vi) Le Fournisseur assistera Kyndryl en fournissant toute information supplémentaire raisonnablement demandée afin de permettre à Kyndryl d'effectuer sa propre évaluation, conformément aux lois applicables relatives à la protection des données en vigueur au Canada, pour déterminer si les Conditions offrent une protection adéquate.

Article III. SÉCURITÉ GÉNÉRALE

3.1. Politiques de Sécurité

- (a) **Politiques.** Les politiques de sécurité de l'information du Fournisseur seront documentées, approuvées par la direction générale du Fournisseur et conformes aux pratiques en vigueur dans le secteur d'activité, telles que celles du National Institute of Standards and Technology (NIST) et/ou de l'Organisation internationale de normalisation (ISO). Les politiques de sécurité de l'information du Fournisseur seront examinées et évaluées par le Fournisseur au moins une fois par an, et rapidement après toute modification importante apportée aux politiques, afin de confirmer qu'elles restent applicables et efficaces. Le Fournisseur ne procédera à aucune modification des politiques qui dégraderait la sécurité du Fournisseur par rapport aux Éléments, aux Livrables ou aux Services de Kyndryl.
- (b) **Tests.** Le Fournisseur mettra en place un processus de tests réguliers de l'efficacité de ses mesures techniques et organisationnelles, afin de garantir la sécurité des Éléments, des Livrables et des Services de Kyndryl.
- (c) **Gestion des risques.** Le Fournisseur effectuera des évaluations des risques de sécurité de l'information appropriées dans le cadre d'un programme de gouvernance des risques continu avec les objectifs suivants : (i) identifier les risques de sécurité de l'information liés aux Éléments, aux Livrables et aux Services de 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 œuvre des mesures pour atténuer et gérer efficacement ces risques en tenant compte du fait que le paysage des menaces évolue constamment.

3.2. Sécurité du personnel

- (a) **Formation à la sécurité.** Au moins une fois par an, le Fournisseur sensibilisera de manière adéquate et fournira une formation appropriées à la sécurité et à la confidentialité à tout le personnel du Fournisseur ayant accès, ou la possibilité d'accéder, aux Éléments, Livrables ou Services de Kyndryl.
- (b) **Vérification des antécédents.** Le Fournisseur maintiendra et appliquera des exigences standard et obligatoires de vérification de l'emploi pour toutes les nouveaux recrutement, et étendra ces exigences à tout son Personnel, ainsi qu'au Personnel des filiales contrôlées par le Fournisseur. Ces obligations comprennent notamment la vérification des antécédents judiciaires dans les limites autorisées par la législation locale, ainsi que la confirmation de l'identité et d'autres contrôles jugés nécessaires par le Fournisseur. Le Fournisseur répétera et revalidera régulièrement ces obligations, s'il le juge nécessaire.

3.3. Gestion des actifs

- (a) **Inventaire des actifs.** Le Fournisseur tiendra un inventaire des actifs de tous les équipements sur lesquels les Éléments de Kyndryl sont stockés. Le Fournisseur limitera l'accès à cet équipement exclusivement au personnel autorisé du Fournisseur. Le Fournisseur empêchera tout accès non autorisé, ainsi que la copie, la modification ou la suppression des Éléments de Kyndryl. Le Fournisseur mettra en place des mesures pour éviter l'accès non autorisé aux Éléments de Kyndryl, leur copie, leur modification ou leur suppression.
- (b) **Sécurité des composants logiciels.** Le Fournisseur s'engage à inventorier de manière appropriée tous les composants logiciels (y compris logiciel open source) utilisés dans la mise à disposition des Services et dans le développement et la mise à disposition des Livrables. Le Fournisseur évaluera si de tels composants logiciels présentent des défauts et/ou des failles de sécurité qui pourraient conduire à la divulgation ou à l'accès non autorisé aux Éléments, Livrables ou Services de Kyndryl. Le Fournisseur effectuera une telle évaluation avant la livraison des Services et des Livrables ou avant de donner à Kyndryl l'accès à ceux-ci, puis de manière continue pendant la durée du Document transactionnel. Le Fournisseur s'engage à corriger en temps opportun tout incident ou toute faille de sécurité dont il aurait connaissance dans les composants logiciels concernés. Le Fournisseur répondra rapidement à toute demande de Kyndryl concernant l'existence d'un défaut ou d'une faille de sécurité dans un tel composant logiciel, qu'ils soient connus du Fournisseur et/ou aient été corrigés par le Fournisseur.

- 3.4. **Politique de contrôle des accès.** Le Fournisseur maintiendra une politique appropriée de contrôle des accès basée sur des rôles et des mesures techniques de contrôle des accès appropriées conformes aux pratiques standard du secteur, afin de restreindre l'accès aux Éléments de Kyndryl et aux actifs du Fournisseur utilisés pour fournir les Services uniquement au personnel autorisé du Fournisseur et de limiter cet accès au niveau le plus bas nécessaire pour fournir et soutenir les Services et les produits Livrables. Ces accès seront conçus conformément aux exigences énumérées au point 3.10(f).

3.5. Autorisation

- (a) Le Fournisseur maintiendra des procédures de création et de suppression de compte utilisateur pour accorder et révoquer rapidement (et dans tous les cas dans les vingt-quatre (24) heures) l'accès à tous les Éléments de Kyndryl et à tous les actifs et applications internes du Fournisseur utilisés dans le cadre de la fourniture des Services et des Livrables. Le Fournisseur désignera une autorité appropriée pour approuver la création et la révocation de comptes utilisateurs ou l'augmentation ou la réduction des niveaux d'accès pour les comptes existants, y compris en cas de cessation d'emploi, de fin de contrat, de mission ou d'autre accord d'un membre du Personnel avec le Fournisseur, ou en cas de changement de rôle si ce membre du Personnel n'a plus besoin de ces droits d'accès.
- (b) Le Fournisseur tiendra à jour et mettra régulièrement à jour les registres des membres du Personnel du Fournisseur autorisés à accéder aux systèmes et aux actifs sur lesquels sont stockés ou à partir desquels peuvent être consultés les Éléments et les Livrables de Kyndryl, ou qui sont utilisés pour fournir les Services, et examinera ces registres au moins tous les trimestres. Le personnel administratif et du support technique ne sera autorisé à accéder à ces systèmes et aux Éléments et aux Livrables de Kyndryl qu'en cas de besoin et à condition que ce personnel se conforme aux mesures techniques et organisationnelles applicables du Fournisseur.
- (c) Le Fournisseur veillera à ce que les comptes utilisateur ayant accès à ces systèmes et actifs soient uniques et restreints par des mots de passe et que les comptes utilisateur ne soient pas partagés.

3.6. Authentification

- (a) Le Fournisseur surveillera les tentatives d'accès répétées aux systèmes d'information et aux actifs.
- (b) Le Fournisseur maintiendra des pratiques de protection des mots de passe conformes aux pratiques standard du secteur et visant à protéger 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 passe complexes et forts et générés de manière aléatoire, ou d'autres alternatives appropriées, telles que des certificats numériques, des cartes/jetons matériels ou des données biométriques.
- (c) Le Fournisseur utilisera l'authentification multifacteur, y compris pour l'accès administratif au domaine et au portail cloud. L'authentification multifacteur peut impliquer des techniques telles que l'utilisation de certificats cryptographiques, de jetons à mot de passe à usage unique (OTP) ou de la biométrie.

3.7. Cryptographie

- (a) **Politique.** Le Fournisseur doit mettre en œuvre et maintenir des politiques et des normes cryptographiques cohérentes avec les pratiques en vigueur dans le secteur d'activité pour protéger les Éléments de Kyndryl, incluant, le cas échéant, la pseudonymisation et le chiffrement.
- (b) **Chiffrement.** Le Fournisseur doit chiffrer les Éléments de Kyndryl en transit et au repos. Les algorithmes de chiffrement protégeront les données à des niveaux de sécurité cohérents avec les pratiques standard du secteur (telles que NIST SP 800-131a) et utiliseront des fonctions de hachage reconnues par le secteur, qui seront au moins aussi protectrices que le chiffrement avancé 256 bits (AES 256) au repos et TLS v1.2 en transit. Le Fournisseur maintiendra et suivra des politiques et des pratiques de gestion des clés cohérentes avec les pratiques standard du secteur, qui définissent les exigences en matière de clés de chiffrement, de sécurité, de rotation et de cycle de vie, incluant 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 des installations à son personnel autorisé.
- (b) **Protection contre les interruptions.** Le Fournisseur prendra les mesures raisonnables pour protéger ces systèmes et actifs contre les pannes d'alimentation électrique et autres perturbations causées par des défaillances des Services publics connexes.
- (c) **Élimination ou réutilisation sécurisée de l'équipement.** Le Fournisseur s'assurera que tous les Éléments de Kyndryl ont été supprimés ou rendus inexploitable sur les équipements contenant des supports de stockage à l'aide de processus conformes aux pratiques standard du secteur avant l'élimination ou la réutilisation de ces équipements.

3.9. Sécurité des opérations

- (a) **Procédures opérationnelles.** Le Fournisseur maintiendra 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 logiciels malveillants.** Le Fournisseur déploiera des solutions antivirus et de gestion des points de terminaison pour maintenir des contrôles contre les logiciels malveillants, afin de protéger ces systèmes et actifs contre les logiciels malveillants, y compris les logiciels malveillants provenant des réseaux publics.
- (c) **Gestion des configurations.** Le Fournisseur disposera de politiques régissant l'installation des logiciels et des utilitaires par le personnel.
- (d) **Gestion des modifications.** Le Fournisseur mettra en place et appliquera des procédures, afin de 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.** En outre, le Fournisseur isolera de manière appropriée ses environnements de production et hors production et tout autre environnement et, si des Éléments de Kyndryl sont déjà présents dans un environnement hors production ou y sont transférés (par exemple pour reproduire une erreur), le Fournisseur veillera à ce que les protections de sécurité et de la confidentialité dans l'environnement hors production soient équivalentes à celles de l'environnement de production.

3.10. Sécurité des communications

- (a) **Transfert d'informations.** Le Fournisseur limitera l'accès par chiffrement aux Éléments de Kyndryl stockés sur des supports qui sont physiquement transportés en dehors des Installations. Le Fournisseur s'assurera qu'il est possible de vérifier et d'établir dans quelle mesure les Éléments de Kyndryl ont été ou peuvent être transmis ou rendus disponibles à l'aide d'équipements de communication de données.
- (b) **Sécurité des Services réseau.** Le Fournisseur veillera à ce que les contrôles et procédures de sécurité soient mis en œuvre pour tous les Services et composants du réseau, conformément aux pratiques en vigueur dans le secteur d'activité, que ces Services soient fournis en interne ou externalisés.
- (c) **Détection des intrusions.** Le Fournisseur déploiera des systèmes de détection ou de prévention d'intrusion, ainsi que des mesures pour prévenir et contrer les attaques par déni de service pour tous les systèmes utilisés pour fournir les Services et les Livrables, y compris une surveillance continue pour intercepter et répondre aux événements de sécurité dès qu'ils sont identifiés, et mettra à jour la base de données des signatures dès que de nouvelles versions sont disponibles pour une distribution commerciale.
- (d) **Pare-feux.** Le Fournisseur mettra en place des pare-feux qui autoriseront uniquement l'utilisation des ports et des Services documentés et approuvés. Tous les autres ports seront placés en mode de « refus total ».
- (e) **Surveillance.** Le Fournisseur surveillera l'utilisation des accès privilégiés et maintiendra des mesures de gestion des informations et des événements de sécurité pour : (i) identifier les accès et activités non autorisés, (ii) faciliter une réponse rapide et appropriée à ces accès et 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-feux, les routeurs, les commutateurs réseau et les systèmes d'exploitation, consistent des informations dans leur journal système respectif ou dans un système de journalisation centralisé, afin d'activer 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 contient des informations confidentielles, (iii) protéger les journaux contre toute modification ou suppression non autorisée, (iv) sauvegarder les journaux quotidiennement, 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 maintiendra et mettra en œuvre des politiques, procédures et normes de développement d'applications sécurisées conformes aux Pratiques standard du secteur, telles que les 25 Techniques de Développement Sécurisé SANS 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 des applications sera qualifié pour fournir les Services et les Livrables et recevra une formation appropriée sur 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 des ports réseau ouverts et inutilisés et la mise en œuvre de systèmes de détection d'intrusions et/ou de systèmes de prévention des intrusions. Les images doivent être validées régulièrement pour mettre à jour leur configuration de sécurité le cas échéant. Le Fournisseur implémentera des outils et des processus correctifs pour les applications et les logiciels système. Lorsque les systèmes obsolètes ne peuvent plus être corrigés, le Fournisseur les mettra à jour avec la dernière version du logiciel d'application. Le Fournisseur supprimera du système les logiciels obsolètes, non pris en charge et inutilisés.
- ii) Le Fournisseur limitera les privilèges d'administration aux seuls membres du personnel qui possèdent à la fois les connaissances nécessaires pour administrer le système d'exploitation et doivent modifier pour des raisons professionnelles la configuration du système d'exploitation sous-jacent.
- (c) **Analyse de la vulnérabilité de l'infrastructure.** Le Fournisseur analysera chaque mois ses environnements internes (par exemple, serveurs, périphériques réseau, etc.) liés aux Services et Livrables, et chaque semaine ses environnements externes liés aux Services et Livrables. Le Fournisseur disposera d'un processus défini et documenté, avec des délais spécifiques, pour traiter les constatations, proportionnellement au risque posé et au niveau de gravité.
- (d) **Évaluation de la vulnérabilité des applications.** Le Fournisseur effectuera une évaluation de la vulnérabilité de la sécurité des applications avant toute nouvelle version publique. Le Fournisseur disposera d'un processus défini et documenté pour traiter toutes les constatations en fonction du risque posé.
- (e) **Tests de pénétration et évaluations de la sécurité.** Le Fournisseur chargera un tiers indépendant reconnu dans le secteur d'activité d'effectuer un test complet de pénétration et une évaluation exhaustive de la sécurité de tous les systèmes impliqués dans la fourniture des Services et des Livrables sur une base récurrente, au moins une fois par an. Le Fournisseur disposera d'un processus défini et documenté pour traiter toutes les constatations 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 effectué par un tiers indépendant a été réalisé et que le Fournisseur a mis en œuvre un processus pour traiter les résultats, conformément à une évaluation des risques. Le Fournisseur fournira un résumé des résultats, comprenant le nombre de systèmes ou applications testés, les dates des tests, la méthodologie des tests et le nombre de constatations critiques, élevées, moyennes et faibles.
- (f) **Reprise après incident.** Pendant la durée du Contrat, le Fournisseur maintiendra une solution de reprise après incident (« DR ») ou à haute disponibilité (« HA ») et un plan connexe pour les Services et Livrables, qui sont cohérents avec les pratiques en vigueur dans le secteur d'activité. Le Fournisseur testera la solution DR ou HA et le plan connexe au moins une fois par an. En outre, la solution et le plan connexe garantiront :
 - i) que les systèmes installés utilisés pour fournir les Services et les Livrables seront restaurés en cas d'interruption,
 - ii) la capacité du Fournisseur à restaurer la disponibilité et accéder aux Éléments de Kyndryl en temps opportun en cas d'incident physique ou technique, et
 - iii) la confidentialité, l'intégrité, la disponibilité et la résilience continues des systèmes que le Fournisseur utilise pour fournir les Services et les Livrables.

3.12. Incidents de Sécurité

- (a) Le Fournisseur suivra et appliquera un programme de réponse aux incidents de sécurité des informations, cohérent avec les pratiques en vigueur dans le secteur d'activité, comprenant des procédures documentées pour analyser et traiter les incidents de sécurité des informations. Le programme de réponse aux incidents de sécurité des informations portera sur des sujets tels que la hiérarchisation des incidents, les rôles et responsabilités, les procédures de remontée, le suivi et la production de rapports, ainsi que le confinement et la remédiation. Le programme de gestion des incidents de sécurité des informations sera testé, examiné et approuvé sur une base périodique, mais au moins une fois par an.
- (b) Le Fournisseur informera rapidement (et en aucun cas plus de 48 heures après) Kyndryl après avoir pris connaissance d'un incident de sécurité en envoyant un courrier électronique à cyber.incidents@kyndryl.com. En cas d'incident de sécurité, le Fournisseur devra agir rapidement pour :
 - i) fournir à Kyndryl les informations raisonnablement demandées concernant cet incident, l'enquête menée par le Fournisseur sur l'incident et l'état d'avancement des activités de remédiation et de restauration du

- Fournisseur. À titre d'exemple, des 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 un accès privilégié, administratif et autre aux périphériques, systèmes, Services ou applications, des résumés basés sur des images contextuelles de périphériques, systèmes ou applications, et d'autres éléments similaires, dans la mesure où ils sont pertinents pour l'incident ou les activités d'atténuation, de résolution et de restauration du Fournisseur ;
- ii) veiller à ce que le personnel approprié du Fournisseur ayant connaissance de l'incident participe aux conférences téléphoniques demandées par Kyndryl ;
 - iii) engager des experts tiers en matière de réponse aux incidents, de gestion des incidents liés aux violations de données, d'investigation et de reconnaissance électronique, à la demande raisonnable de Kyndryl ;
 - iv) fournir à Kyndryl une assistance raisonnable pour remplir toutes les obligations légales (y compris les obligations d'avertir les régulateurs, les personnes concernées, le client ou autre tiers) de Kyndryl, des sociétés affiliées de Kyndryl et des clients (et de leurs clients et sociétés affiliées) ; et
 - v) résoudre de manière opportune et adéquate les 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 concernant ces mesures correctives et cette résolution.
- (c) Le Fournisseur est responsable de tous les coûts et dépenses engagés par le Fournisseur pour enquêter, répondre à, atténuer et remédier à un incident de sécurité. Sous réserve de la limitation de responsabilité dans l'Accord, le Fournisseur est également responsable de tous les coûts et dépenses engagés par Kyndryl, les sociétés affiliées de Kyndryl et les Clients (ainsi que leurs clients et affiliés) en lien avec l'enquête, la réponse, l'atténuation et la résolution de l'Incident de Sécurité. Les coûts et dépenses de remédiation d'un Incident de Sécurité peuvent inclure les coûts liés à la détection et à l'investigation d'un Incident de Sécurité, à la détermination des responsabilités en vertu des lois et réglementations, au rechargement des données, à la correction des défauts de produit (y compris via le Code Source ou d'autres développements), au recours à des tiers pour aider aux activités mentionnées ci-dessus ou à d'autres activités pertinentes, ainsi qu'à d'autres coûts et dépenses nécessaires pour remédier aux effets néfastes de l'Incident de sécurité.
- (d) En cas d'incident de sécurité impliquant des Données à caractère personnel de Kyndryl, le Fournisseur est responsable de tous les coûts engagés et remboursera Kyndryl pour tous les coûts et dépenses supportés par Kyndryl relatifs à ce qui suit :
- i) Notification de l'incident de sécurité aux autorités de réglementation compétentes, à d'autres agences d'autorégulation gouvernementales et sectorielles, aux médias (si la législation applicable l'exige), aux personnes concernées, aux clients et à d'autres personnes ;
 - ii) Mise en place et maintien d'un centre d'appels pour répondre aux questions des personnes concernées sur l'incident de sécurité et ses conséquences, pendant 1 année 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 autres éléments à utiliser par le personnel du centre d'appels lors de la réponse aux demandes de renseignements concernant les Données à caractère personnel de Kyndryl ; et
 - iii) Fourniture des services de protection contre le vol d'identité, de surveillance du crédit et de restauration du crédit pendant 2 ans après la date à laquelle les Personnes concernées affectées par l'incident, ayant 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 affecté par un Incident de sécurité, à moins que Kyndryl ne l'accepte par écrit ou que la loi ne l'exige. Le Fournisseur avertira Kyndryl par écrit avant de diffuser toute notification requise par la loi à un tiers, celle-ci étant de nature à révéler directement ou indirectement l'identité de Kyndryl.
- (f) Le Fournisseur notifiera également rapidement à Kyndryl toute menace réelle ou imminente de violation des présentes conditions ou de ses politiques de sécurité, procédures de sécurité ou politiques d'utilisation acceptable liées à la livraison d'un Livrable ou la fourniture des Services.

3.13. Relations avec les fournisseurs

- (a) **Sous-traitants.** Le Fournisseur est responsable du respect de ces conditions, même s'il a recours à un Sous-traitant. Le Fournisseur s'engage contractuellement à ce que ces Sous-traitants protègent les Éléments de Kyndryl dans des conditions qui ne sont pas moins complètes ou rigoureuses que celles qui s'appliquent au

fournisseur dans les conditions. Le Fournisseur est responsable envers Kyndryl de la performance de chaque Sous-traitant.

- (b) **Contrôle de qualité et gestion de la sécurité.** Le Fournisseur effectuera le contrôle de qualité et la supervision de la gestion de la sécurité du développement de logiciels externalisé à un Sous-traitant.
- (c) **Informations précontractuelles.** Le Fournisseur déclare et garantit que toutes les informations matérielles fournies au cours des discussions précontractuelles avec Kyndryl concernant la confidentialité, la sécurité et la gouvernance des données, que ce soit en vertu des présentes conditions ou autrement, sont exactes dans tous les aspects matériels et ne sont pas, que ce soit par omission ou autrement, trompeuses.

3.14. Vérification, coopération, conformité et évaluation de la sécurité

- (a) **Vérification** Le Fournisseur tiendra à jour un registre pouvant faire l'objet d'un audit et démontrant son respect des présentes Conditions.
 - (i) L'entreprise Kyndryl, seule ou avec un auditeur externe, est autorisée, dans les trente (30) Jours suivant un préavis écrit adressé au fournisseur, à vérifier la conformité du Fournisseur aux présentes Conditions, notamment en accédant à une ou plusieurs Installations à de telles fins. L'entreprise Kyndryl n'accédera à aucun centre de données dans lequel le Fournisseur traite les Données de Kyndryl, sauf si elle estime de bonne foi que cela fournirait des informations pertinentes. Le Fournisseur coopérera à la vérification de Kyndryl, notamment en répondant dans les délais et en intégralité aux demandes d'informations, par le biais de documents, d'autres registres, d'entretiens avec le Personnel concerné du Fournisseur, etc. Le Fournisseur peut apporter la preuve de son adhésion à un code de conduite approuvé ou à une certification agréée dans le Secteur d'Activité, ou fournir à Kyndryl toute autre information démontrant le respect des présentes Conditions, à des fins de vérification par Kyndryl.
 - (ii) Une vérification n'aura pas lieu plus d'une fois sur une période de 12 mois, sauf si : (A) Kyndryl valide la remédiation par le Fournisseur des problèmes résultant d'une vérification précédente pendant la période de 12 mois, ou (B) un Incident de sécurité survient et Kyndryl souhaite vérifier le respect des obligations liées à l'incident. Dans les deux cas, Kyndryl fournira le même préavis écrit de 30 jours que celui spécifié au paragraphe (i) ci-dessus, mais l'urgence de traiter un Incident de sécurité peut nécessiter que Kyndryl effectue une vérification avec un préavis écrit de moins de 30 jours.
 - (iii) Un régulateur ou, lorsqu'il y est légalement autorisé, un autre Responsable du traitement peut exercer les mêmes droits que Kyndryl aux paragraphes (ii) et (iii), étant entendu qu'un régulateur peut exercer tout droit supplémentaire que la loi lui confère.
 - (iv) Si Kyndryl dispose d'arguments raisonnables permettant de conclure que le Fournisseur ne respecte pas l'une des présentes Conditions (que ces arguments proviennent d'une vérification effectuée au titre des présentes Conditions ou d'une autre façon), le Fournisseur devra rapidement remédier à cette non-conformité.
 - (v) La présente section s'appliquera en plus de la clause « Tenue de registres et droit d'audit » ou toute autre clause d'audit similaire dans l'Accord.
- (b) **Coopération.** Si Kyndryl a des raisons de s'interroger sur le fait que des Services ou des Livrables ont pu contribuer, contribuent ou contribueront à un problème de cybersécurité, le Fournisseur coopérera de manière raisonnable à toute enquête de Kyndryl concernant ce problème, y compris en répondant de manière rapide et complète aux demandes d'informations, que ce soit par des documents, d'autres enregistrements, des entretiens avec le Personnel concerné du Fournisseur, ou des moyens similaires.
- (c) **Conformité en matière de sécurité.** Le Fournisseur obtiendra (i) une certification de conformité à la norme ISO 27001, d'une entreprise de contrôle public indépendant, (ii) un rapport d'une entreprise de contrôle public indépendant démontrant son examen des systèmes, des contrôles et des opérations du Fournisseur conformément à un SOC 2 de Type 2, qui inclura au minimum les Principes de Sécurité du Service de Confiance (également connu sous le nom de Critères Communs), la Disponibilité et la Confidentialité, et (iii) un rapport d'une entreprise de contrôle public indépendant démontrant son examen des systèmes, des contrôles et des opérations du Fournisseur conformément à un SOC 1 de Type 2, si les Services ont un impact sur les rapports financiers de Kyndryl. Le Fournisseur se conformera aux futures orientations relatives à la norme SSAE18 publiées par l'AICPA, l'IAASB, la Securities and Exchange Commission ou la Public Company Accounting. Sur demande, le Fournisseur fournira rapidement à Kyndryl une copie de chaque certificat et rapport 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 Livrable individuel, le Fournisseur devra compléter avec

précision et dans les délais (ne dépassant pas 14 jours) un questionnaire pour vérifier la conformité du Fournisseur à ses obligations en matière de cybersécurité et de gouvernance des données en vertu de l'Accord et des présentes conditions (« **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 gouvernance des données ne répondent 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, il devra, sans délai déraisonnable : (i) corriger ces lacunes à ses propres frais dans un délai convenu avec Kyndryl sur la base d'une évaluation du risque ; et (ii) fournir à Kyndryl, ou à ses représentants dûment autorisés, une documentation et des informations raisonnables confirmant la correction des lacunes. Si le Fournisseur ne remédie pas à des lacunes importantes ou critiques dans les délais convenus, Kyndryl a le droit de dénoncer le Document de Transaction applicable ou l'Accord pour violation substantielle immédiatement après en avoir avisé le Fournisseur. Kyndryl ne divulguera pas la documentation à une tierce partie autre que ses propres auditeurs sans le consentement écrit du Fournisseur. Si le Fournisseur n'est pas d'accord avec l'évaluation des lacunes par Kyndryl, il fournira rapidement à Kyndryl une explication écrite détaillant ses raisons, et si Kyndryl n'accepte pas les raisons du Fournisseur, les parties feront appel à leur responsable de la protection de la confidentialité, à leur responsable de la sécurité de l'information ou à un responsable ayant des prérogatives et une autorité similaires, afin de trouver une solution dans les meilleurs délais. Si des déficiences sont causées par l'utilisation des Services par Kyndryl, le Fournisseur fournira une assistance technique raisonnable pour aider Kyndryl à utiliser les Services de manière appropriée, afin de remédier à ces déficiences.

Article IV. ACCÈS AUX RÉSEAUX KYNDRYL

Le présent Article s'applique si les employés du Fournisseur vont avoir accès à un Système d'Entreprise.

4.1. Conditions Générales

- (a) Kyndryl déterminera si les employés du Fournisseur seront autorisés à accéder aux Systèmes d'entreprise. Si Kyndryl accorde cette autorisation, le Fournisseur devra se conformer et s'assurer que ses employés disposant dudit accès se conforment aux exigences du présent Article.
- (b) Kyndryl déterminera les moyens permettant aux employés du Fournisseur d'accéder aux Systèmes d'entreprise, notamment si ces employés auront accès aux Systèmes d'entreprise par le biais de Périphériques fournis par Kyndryl ou par le Fournisseur.
- (c) Les employés du Fournisseur ne peuvent accéder qu'aux systèmes de l'entreprise et ne peuvent utiliser que les Périphériques de Kyndryl que Kyndryl autorise pour cet accès, afin de fournir des Services, qui seront soit un périphérique fourni par Kyndryl (« Périphérique de Kyndryl »), soit un appareil fourni par le Fournisseur (« Périphérique du Fournisseur »).
- (d) Les employés du Fournisseur ne copieront pas les Éléments de Kyndryl accessibles par le biais d'un Système d'Entreprise, sans l'Accord préalable écrit de Kyndryl (et ne copieront jamais les Éléments de Kyndryl sur un périphérique de stockage portable tel qu'une clé USB, un disque dur externe ou autres éléments similaires).
- (e) Sur demande, le Fournisseur indiquera les Systèmes d'entreprise spécifiques auxquels chaque employé est autorisé à accéder et auxquels il a accédé sur une période définie par Kyndryl.
- (f) Le Fournisseur notifiera à Kyndryl dans un délai de vingt-quatre (24) heures qu'un employé du Fournisseur ayant accès à un Système d'entreprise : (i) n'est plus employé par le Fournisseur, (ii) n'exerce plus les activités nécessitant ledit accès. Le Fournisseur collaborera avec Kyndryl pour veiller à ce que l'accès accordé à ces employés ou anciens employés soit immédiatement révoqué.
- (g) Le Fournisseur signalera immédiatement à Kyndryl tous les incidents de sécurité réels ou présumés (par exemple, perte d'un Périphérique de Kyndryl ou du Fournisseur ou accès non autorisé à un Périphérique ou aux données, éléments ou autres informations de quelque nature que ce soit) et coopérera avec Kyndryl à l'enquête sur de tels incidents.
- (h) Le Fournisseur ne doit autoriser aucun employé d'un agent, entrepreneur indépendant ou sous-traitant à accéder aux Systèmes d'entreprise sans l'Accord préalable écrit de Kyndryl ; si Kyndryl donne cet accord, le Fournisseur engagera contractuellement ces personnes et leurs employeurs à respecter les exigences du présent Article comme si ces personnes étaient des employés du Fournisseur, et sera responsable vis-à-vis de Kyndryl de toutes les actions et omissions de ces personnes ou employeurs en lien avec ledit accès aux Systèmes d'entreprise.
- (i) Kyndryl pourra à tout moment révoquer l'accès physique aux Systèmes d'entreprise, pour tout employé du Fournisseur ou pour l'ensemble du personnel du Fournisseur, sans notification préalable au fournisseur ou à tout employé ou autre agent du Fournisseur, si Kyndryl estime que cela est nécessaire pour protéger Kyndryl.
- (j) Les droits de Kyndryl ne sont pas bloqués, réduits ou restreints de quelque manière que ce soit par une disposition du Document Transactionnel, de l'accord de base associé entre les parties, ou de tout autre accord entre les parties, y compris toute disposition qui pourrait exiger que des données, des documents ou d'autres informations de quelque nature que ce soit résident uniquement dans un ou plusieurs emplacements spécifiques, ou qui pourrait exiger que seules des personnes d'un ou plusieurs emplacements spécifiques accèdent à ces données, documents ou autres informations

4.2. Logiciel de périphérique

- (a) Le Fournisseur demandera à son personnel d'installer en temps utile sur les Périphériques de Kyndryl et les Périphériques du Fournisseur les logiciels dont Kyndryl a besoin pour faciliter l'accès aux systèmes de l'entreprise de manière sécurisée. Ni le Fournisseur, ni son personnel n'interféreront dans les opérations de ce logiciel ou les dispositifs de sécurité activés par le logiciel.
- (b) Le Fournisseur et son personnel respecteront les règles de configuration des Périphériques de Kyndryl et des Périphériques du Fournisseur établies par Kyndryl et collaboreront avec Kyndryl afin de garantir que le logiciel fonctionne comme Kyndryl l'entend. Par exemple, le Fournisseur n'est pas autorisé à contourner les fonctions de blocage de site Web ou d'application automatisée de correctifs.
- (c) Le personnel du Fournisseur ne doit pas partager avec d'autres personnes les noms d'utilisateur, les mots de passe ou autres pour les Périphériques de Kyndryl et les Périphériques du Fournisseur.
- (d) Si Kyndryl autorise le personnel du Fournisseur à accéder aux Systèmes d'entreprise à l'aide des Périphériques du Fournisseur, ce dernier installera et exécutera sur ces Périphériques un système d'exploitation approuvé par Kyndryl et mis à niveau vers une nouvelle version de ce système d'exploitation ou d'un nouveau système d'exploitation dans un délai raisonnable suivant les instructions de Kyndryl.

4.3. Périphériques de Kyndryl

- (a) Les employés du Fournisseur ne peuvent pas utiliser les Périphériques de Kyndryl pour fournir des Services à toute autre personne ou entité, ou pour accéder à des systèmes informatiques, réseaux, applications, sites Web, outils de messagerie électronique, outils de collaboration, etc. du Fournisseur ou d'un tiers pour ou en liaison avec les Services. Les employés du Fournisseur ne peuvent pas utiliser les Périphériques de Kyndryl pour des raisons personnelles (par exemple, les employés du Fournisseur ne peuvent pas stocker des fichiers personnels tels que de la musique, des vidéos, des images ou d'autres éléments similaires sur ces Périphériques de Kyndryl et ne peuvent pas utiliser Internet à partir desdits périphériques pour des motifs personnels). Les employés du Fournisseur ne peuvent pas partager les Périphériques de Kyndryl avec d'autres employés du Fournisseur qu'ils utilisent pour accéder aux systèmes d'entreprise.
- (b) Kyndryl a le droit absolu de surveiller et de remédier aux intrusions potentielles et autres menaces de cybersécurité de quelque manière que ce soit, depuis n'importe quel endroit et en utilisant tout moyen que Kyndryl juge nécessaire ou approprié, sans préavis au fournisseur ou à un employé du Fournisseur ou autre. Exemples de ces droits : Kyndryl pourra à tout moment (i) mener un test de sécurité sur n'importe quel Périphérique, (ii) surveiller, restaurer par des moyens techniques ou autres et passer en revue les communications (notamment les e-mails provenant de n'importe quel compte de messagerie), enregistrements, fichiers et autres éléments stockés sur un Périphérique ou transmis par le biais d'un Système d'entreprise et (iii) se procurer une image contextuelle complète de tout Périphérique. Si Kyndryl a besoin de la coopération du Fournisseur pour exercer ses droits, le Fournisseur répondra entièrement et dans les délais convenus aux demandes de coopération de Kyndryl (par exemple, aux demandes de configuration sécurisée d'un Périphérique, d'installation d'un logiciel de surveillance ou autre sur un Périphérique, de partage des détails de connexion de niveau système, de mise en œuvre de mesures d'intervention en cas d'incident sur un Périphérique et d'octroi de l'accès physique ou autre à un Périphérique, afin que Kyndryl puisse obtenir une image contextuelle complète, ainsi que des demandes similaires et connexes).
- (c) Kyndryl conservera la propriété de tous les Périphériques de Kyndryl dont le risque de perte, notamment par suite de vol, vandalisme ou négligence, sera assumé par le Fournisseur. Le Fournisseur n'apportera ou ne permettra aucune altération des Périphériques de Kyndryl sans l'Accord préalable écrit de Kyndryl, le terme altération désignant toute modification d'un Périphérique, y compris des logiciels, applications, conceptions de sécurité, configurations de paramètres de sécurité ou la conception physique, mécanique ou électrique d'un Périphérique.
- (d) Le Fournisseur restituera tous les Périphériques de Kyndryl dans les cinq (5) jours ouvrables après que ces Périphériques ne sont plus nécessaires pour la fourniture des Services et détruira en même temps, à la demande de Kyndryl, l'ensemble des données, éléments ou autres informations de quelque nature que ce soit sur ces Périphériques, sans en conserver de copie, conformément aux normes NIST relatives à la suppression définitive de tous ces éléments, données ou autres informations. Le Fournisseur devra, à ses frais, conditionner les Périphériques de Kyndryl et les retourner dans le même état que celui dans lequel ils ont été livrés au fournisseur, exception faite de l'usure normale, au site défini par Kyndryl. Le manquement du Fournisseur à toute obligation du présent paragraphe (d) constitue une violation substantielle du Document de Transaction et de l'Accord de base associé et de tout Contrat connexe entre les parties, étant entendu qu'un contrat est « connexe » si l'accès à un Système d'entreprise facilite les tâches ou autres activités du Fournisseur au titre de cet Accord.
- (e) Kyndryl fournira un service de support pour les Périphériques de Kyndryl (notamment l'inspection et la maintenance préventive et corrective des Périphériques). Le Fournisseur avisera Kyndryl sans délai de la nécessité d'un service de maintenance corrective.
- (f) Pour les logiciels dont Kyndryl est propriétaire ou qu'elle a le droit de concéder sous licence, Kyndryl confère au fournisseur un droit temporaire permettant de les utiliser, de les stocker et d'en faire suffisamment de copies aux fins de l'utilisation autorisée des Périphériques de Kyndryl. Le Fournisseur n'est pas autorisé à transférer les logiciels à quiconque, à faire des copies des informations de licence logicielle, ni à désassembler, décompiler, traduire de quelque façon que ce soit un logiciel ou avoir recours à l'ingénierie inverse, à moins d'y être expressément autorisé par la législation applicable interdisant toute disposition légale contraire.

Article V. DÉFINITIONS

Les termes « Services » et « Livrables » sont probablement définis dans l'Accord de relation fournisseur ou dans un Document de Transaction équivalent, mais s'ils ne le sont pas, alors « **Services** » désigne tout hébergement, conseil, installation, personnalisation, maintenance, support, extension du personnel, travail commercial, technique ou autre

que le Fournisseur effectue pour Kyndryl, comme spécifié dans le Document de Transaction, et « **Livrables** » désigne tous les programmes logiciels, plateformes, applications ou autres produits ou articles et les éléments connexes respectifs que le Fournisseur fournit à Kyndryl, comme spécifié dans le Document de Transaction.

- 5.1. **Pays adéquat** désigne un pays fournissant un niveau suffisant de protection des données concernant le transfert concerné, conformément aux lois applicables en matière de protection des données ou aux décisions des régulateurs.
- 5.2. **Système d'IA** désigne un système automatisé conçu pour fonctionner avec différents niveaux d'autonomie et pouvant faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, comment générer des données de sortie telles que des prédictions, du contenu, des recommandations ou des décisions pouvant influencer des environnements physiques ou virtuels.
- 5.3. **Coordonnées professionnelles** (« **CP** ») désigne les Données à caractère personnel utilisées pour prendre contact avec une personne physique, l'identifier ou l'authentifier à titre professionnel ou commercial à des fins de gestion administrative et de gestion des contrats (par exemple, facturation et gestion des comptes, calcul des primes des partenaires, reporting interne et modélisation métier telle que les prévisions, la planification des revenus et des capacités), et à nulle autre fin. En général, les Coordonnées professionnelles comprennent le nom, l'adresse électronique professionnelle, l'adresse postale, le numéro de téléphone ou les informations similaires relatives à un individu. Par exemple, les noms et les adresses électroniques utilisés pour contacter le personnel du Fournisseur pour les Services d'assistance sont des coordonnées professionnelles, tandis que les noms et adresses électroniques inclus dans les données d'assistance aux diagnostics sont des Données à caractère personnel de Kyndryl.
- 5.4. **Service Cloud** désigne toute offre « en tant que service » hébergée ou gérée par le Fournisseur, y compris les offres de « logiciel en tant que de service », de « plateforme en tant que service » et « d'infrastructure en tant que service ».
- 5.5. **Responsable de traitement** désigne une personne physique ou morale, une autorité publique, une agence ou tout autre organisme déterminant, seul ou conjointement avec d'autres entités, les finalités et moyens du Traitement des Données à caractère personnel.
- 5.6. **Système d'entreprise** désigne un système, une plateforme, une application, un réseau informatique ou un autre système similaire sur lequel Kyndryl s'appuie pour ses activités, y compris ceux situés sur ou accessibles en utilisant l'intranet de Kyndryl, Internet ou d'autres moyens.
- 5.7. **Client** désigne un client de Kyndryl.
- 5.8. **Importateur de données** signifie Processeur des données ou Sous-traitant des données non 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 les jours civils, à moins que l'adjectif « ouvrable » ne soit associé à ce terme.
- 5.11. **Périphérique** désigne un poste de travail, un ordinateur portable, une tablette, un smartphone ou un assistant numérique personnel fourni par Kyndryl ou par le Fournisseur.
- 5.12. **Installations** désigne un emplacement physique où le Fournisseur héberge aux Livrables ou les Documents de Kyndryl, y accède ou les traite d'une manière ou d'une autre.
- 5.13. **Pratiques standard du secteur** désigne les pratiques recommandées ou exigées par le National Institute of Standards and Technology (« **Institut national de la statistique (INST)** ») ou l'Organisation internationale de normalisation (« **ISO** »), ou tout autre institution ou organisation de réputation et de sophistication similaires.
- 5.14. **Données de Kyndryl** signifie toutes les données, fichiers, éléments, textes, sons, vidéos, images ou autres données, y compris les Données personnelles de Kyndryl, les Coordonnées professionnelles de Kyndryl et les Données non personnelles de Kyndryl, qui sont fournies au Fournisseur (y compris, sans limitation, via un Service de Cloud) dans le cadre de la fourniture de Services ou d'un Livrable, que ce soit fourni ou rendu accessible par Kyndryl, le Personnel de Kyndryl, un Client, un employé ou un sous-traitant du Client, ou toute autre personne ou entité.
- 5.15. **Documents de Kyndryl** désigne toutes les Données de Kyndryl et la Technologie de Kyndryl.
- 5.16. **Données personnelles de Kyndryl** désigne les Données personnelles, à l'exclusion des Coordonnées professionnelles de Kyndryl, que Kyndryl fournit ou rend accessible au fournisseur pour la fourniture des Services ou des Livrables. Les Données à caractère personnel de Kyndryl incluent les Données personnelles que Kyndryl contrôle ou celles que Kyndryl traite au nom d'autres Responsables du traitement.
- 5.17. **Technologie de Kyndryl** désigne le Code source, le reste du code, les descriptions, les microprogrammes, les logiciels, les outils, les conceptions, les schémas, les représentations graphiques, les clés intégrées, les certificats et les autres informations, éléments, actifs, documents et technologies de Kyndryl que Kyndryl a

- directement ou indirectement concédés sous licence ou transmis au fournisseur en lien avec le Document de Transaction ou un contrat connexe entre Kyndryl et le Fournisseur.
- 5.18. **Pays non adéquat** désigne un pays qui n'est pas jugé adéquat conformément aux lois applicables en matière de protection des données ou à une décision d'un régulateur compétent.
- 5.19. **Autres responsables du traitement** désigne toute entité autre que Kyndryl, qui est un Responsable du traitement de Données de Kyndryl, par exemple, une société affiliée de Kyndryl, un Client ou une société affiliée du Client.
- 5.20. **Le logiciel sur site** désigne le logiciel fourni par le Fournisseur en tant que 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 « donnée personnelle » ou similaire au titre de toute loi sur la protection des données.
- 5.22. **Personnel** désigne les personnes qui sont des employés de Kyndryl ou du Fournisseur, des agents de Kyndryl ou du Fournisseur, des entrepreneurs indépendants engagés par Kyndryl ou le Fournisseur, ou mis à la disposition d'une partie par un Sous-traitant.
- 5.23. **Traiter** ou **Traitement** signifie toute opération ou tout ensemble d'opérations effectuées sur les Données de Kyndryl, y compris stockage, utilisation, accès et lecture.
- 5.24. **Processeur** désigne une personne physique ou morale qui traite des données à caractère personnel pour le compte d'un responsable du traitement et comprend le « fournisseur de Services » ou des termes substantiellement similaires en vertu de toute loi sur la protection des données.
- 5.25. **Incident de sécurité** désigne (a) un événement qui compromet ou menace de compromettre la confidentialité, l'intégrité ou la disponibilité des Éléments Kyndryl ou d'un système d'information utilisé par le Fournisseur ou ses Sous-traitants pour fournir les Services ou les Livrables, (b) une violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès aux Données de Kyndryl transmises, stockées ou traitées de toute autre manière, 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 de Services ou de Livrables ou en rapport avec celle-ci.
- 5.26. **Vendre** (ou **Vente**) désigne la vente, la location, le lancement, la divulgation, la diffusion, la mise à disposition, le transfert ou toute autre communication verbale, écrite ou électronique ou par tout autre moyen, des données contre rémunération ou contre toute autre contrepartie de valeur.
- 5.27. **Partager** a le sens qui lui est donné 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 applicables sur la protection des données pour le transfert des Données à caractère personnel aux Responsables du traitement et aux processeurs de données non établis dans des Pays adéquats.
- 5.29. **Code Source** désigne un code de programmation lisible par l'homme ou un code pouvant être converti en forme lisible par l'homme que les développeurs utilisent pour créer, développer ou maintenir un produit, mais qui n'est pas rendu public dans le cours normal de la distribution ou de l'utilisation commerciale du produit.
- 5.30. **Sous-traitant des données** désigne tout sous-traitant du Fournisseur, y compris une société affiliée du Fournisseur, qui traite des Données de Kyndryl.
- 5.31. **Autorité de surveillance** désigne un organisme public indépendant chargé de surveiller l'application des lois sur la protection des données au sein d'un pays ou d'une région spécifique.