Article I, Coordonnées professionnelles

Cet Article s'applique si le Fournisseur ou Kyndryl Traite les Coordonnées professionnelles de l'autre.

1.1 Kyndryl et le Fournisseur peuvent Traiter les Coordonnées professionnelles de l'autre partie, quel que soit l'endroit où ils exercent leurs activités, dans le cadre de la fourniture des Services et Livrables par le Fournisseur.

1.2 Les partie s'engagent :

(a) à ne pas utiliser ou divulguer les Coordonnées professionnelles de l'autre partie à d'autres fins (pour plus de clarté, aucune partie ne pourra Vendre les Coordonnées professionnelles de l'autre partie ou utiliser ou divulguer les Coordonnées professionnelles de l'autre partie à des fins de marketing sans l'accord préalable écrit de l'autre partie et, le cas échéant, l'accord préalable écrit des Personnes concernées) et

(b) à supprimer, modifier, corriger, renvoyer, fournir les informations sur le Traitement, restreindre le Traitement, ou prendre toute autre mesure raisonnablement demandée au regard des BCI de l'autre partie, sans délai sur demande écrite de l'autre partie, chaque fois qu'une utilisation non autorisée des informations personnelles aura lieu, et que la partie voudra arrêter le traitement et corriger.

1.3 Les parties n'établissent pas de relation à titre de Responsable de traitement conjoint en ce qui concerne leurs Coordonnées professionnelles, et aucune condition du Document de Transaction ne sera interprétée comme indiquant l'intention d'établir une relation à titre de Responsable de traitement conjoint.

1.4 La Déclaration de Confidentialité de Kyndryl à l'adresse https://www.kyndryl.com/us/en/privacy contient des informations supplémentaires sur le Traitement des BCI par Kyndryl.

1.5 Les parties ont mis en place et respecteront des mesures de sécurité techniques et organisationnelles pour protéger les Coordonnées professionnelles de l'autre partie contre la perte, la destruction, la modification, la divulgation accidentelle ou non autorisée, l'accès accidentel ou non autorisé ou le Traitement illégal.

1.6 Le Fournisseur s'engage à avertir Kyndryl dans les meilleurs délais (et au plus tard dans les 48 heures) après avoir pris connaissance de toute Violation de Sécurité impliquant les Coordonnées professionnelles de Kyndryl. Le Fournisseur enverra cette notification à l'adresse cyber.incidents@kyndryl.com. Le Fournisseur fournira à Kyndryl toute information raisonnablement demandée sur cette violation et sur le statut de toute activité de résolution et de restauration du Fournisseur. À titre d'exemple, les informations raisonnablement demandées peuvent inclure des historiques démontrant un accès privilégié, administratif et autre aux appareils, aux systèmes ou aux applications, des images d'appareils, de systèmes ou d'applications, et d'autres éléments similaires, dans la mesure pertinente à la résolution de la violation ou des activités de réparation ou de restauration du Fournisseur.

1.7 Si le Fournisseur ne Traite que les Coordonnées professionnelles de Kyndryl et qu'il n'a accès à aucun autre élément ou donnée d'aucune sorte ou à aucun Système d'entreprise de Kyndryl, le présent Article et l'Article X (Coopération, Vérification et Résolution) sont les seuls Articles applicables audit Traitement.

Article II, Mesures Techniques et Organisationnelles, Sécurité des Données

Le présent Article s'applique si le Fournisseur Traite des Données de Kyndryl autres que les Coordonnées professionnelles de Kyndryl. Le Fournisseur doit respecter les obligations du présent Article en fournissant tous les Services et Livrables et ainsi protéger les Données de Kyndryl contre toute perte, destruction, modification, divulgation accidentelle ou non autorisée, accès accidentel ou non autorisé et toute autre forme illégale de Traitement. Les obligations énoncées dans le présent Article s'appliquent à toutes les applications, plateformes et infrastructures informatiques que le Fournisseur exploite ou gère lors de la fourniture des Livrables et Services, y compris tous les développements, tests, hébergements, supports, opérations et environnements de centre de données.

1. Utilisation des Données

1.1 Le Fournisseur n'est pas autorisé à ajouter des données aux Données de Kyndryl, ou à inclure aux Données de Kyndryl d'autres informations ou données, y compris des Données à caractère Personnel, sans l'accord préalable écrit de Kyndryl. Le Fournisseur n'est pas autorisé à utiliser les Données de Kyndryl sous toute forme, agrégée ou autre, à toute autre fin que celle de livrer les Services et Livrables (par exemple, le Fournisseur n'est pas autorisé à utiliser ou réutiliser les Données de Kyndryl pour évaluer l'efficacité des offres du Fournisseur ou le moyen de les améliorer, à des fins de recherche et de développement pour créer de nouvelles offres ou pour générer des rapports sur les offres du Fournisseur). À moins d'y être expressément autorisé dans le Document de Transaction, le Fournisseur n'a pas le droit de Vendre les Données de Kyndryl.

1.2 Le Fournisseur s'engage à ne pas intégrer de technologies de suivi Web aux Livrables ou dans le cadre des Services (ces technologies incluent HTML5, le stockage local, les balises ou jetons tiers et les pixels espions), à moins d'y être expressément autorisé dans le Document de Transaction.

2. Demandes émanant de tiers et confidentialité

2.1 Le Fournisseur s'engage à ne divulguer les Données de Kyndryl à aucun tiers, sauf accord préalable écrit de Kyndryl. Si un gouvernement, y compris une autorité de régulation, exige l'accès aux Données de Kyndryl (par exemple, si le gouvernement des États-Unis signifie au Fournisseur une ordonnance de sécurité nationale pour obtenir les Données de Kyndryl) ou si une divulgation des Données de Kyndryl est exigée par la loi, le Fournisseur est tenu de notifier par écrit à Kyndryl ladite demande ou obligation de divulgation afin que Kyndryl ait la possibilité de la contester (lorsque la loi interdit la notification, le Fournisseur prendra les mesures qu'il estime raisonnablement appropriées pour contester la divulgation des Données de Kyndryl par le biais d'une action judiciaire ou d'autres moyens).

2.2 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 pour fournir ces Services et Livrables ; 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.

3. **Restitution ou suppression des Données de Kyndryl**

3.1 Le Fournisseur supprimera ou restituera, au choix de Kyndryl, les Données de Kyndryl 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 aux Bonnes pratiques du secteur, à rendre les données illisibles et impossibles à réassembler ou à reconstituer et certifiera à Kyndryl la suppression. Si Kyndryl exige la restitution des Données de Kyndryl, le Fournisseur les restituera dans les délais raisonnables prévus par Kyndryl et selon les instructions écrites raisonnables de Kyndryl.

Article III, Confidentialité

Le présent Article s'applique si le Fournisseur Traite des Données à caractère personnel de Kyndryl.

1. Traitement

1.1 Kyndryl désigne le Fournisseur comme Sous-traitant chargé de Traiter les Données à caractère personnel de Kyndryl dans le seul but de fournir les Livrables et Services conformément aux instructions de Kyndryl, y compris celles figurant dans les présentes Conditions, le Document de Transaction et le contrat de base associé entre les parties. Si le Fournisseur ne se conforme pas à une instruction, Kyndryl peut résilier la partie affectée des Services en le notifiant par écrit. 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. Si le Fournisseur ne respecte pas l'une de ses obligations en vertu des présentes Conditions et que ce manquement entraîne une utilisation non autorisée d'Informations personnelles, ou, de façon générale, dans tous les cas d'utilisation non autorisée d'Informations personnelles, Kyndryl aura le droit d'arrêter le traitement, de corriger au manquement et de remédier aux effets préjudiciables de l'utilisation non autorisée, selon les instructions et les délais raisonnables de Kyndryl.

1.2 Le Fournisseur s'engage à respecter toutes les lois sur la protection de données applicables aux Services et Livrables.

1.3 Une Annexe au Document de Transaction, ou le Document de Transaction lui-même, indique les points suivants en ce qui concerne les Données de Kyndryl :

(a) les catégories de Personnes Concernées ;
(b) les types de Données à caractère personnel de Kyndryl ;
(c) les actions sur les données et les activités de Traitement des données ;
(d) la durée et la fréquence du Traitement ; et
(e) la liste des Sous-traitants ultérieurs.

2. Mesures Techniques et Organisationnelles

2.1 Le Fournisseur s'engage à mettre en place et à tenir à jour les mesures techniques et organisationnelles décrites à l'Article II (Mesures Techniques et Organisationnelles, Sécurité des Données) et à l'Article VIII (Mesures Techniques et Organisationnelles, Sécurité Générale) et, ce faisant, à assurer un niveau de sécurité adapté au risque présenté par ses Services et Livrables. Le Fournisseur certifie et comprend les restrictions énoncées à l'Article II, au présent Article III et à l'Article VIII et devra s'y conformer.

3. Droits et Demandes des Personnes Concernées

3.1 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 de d'exercer ses droits (tels que son droit à rectification, suppression ou 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.

3.2 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 planning permettant à Kyndryl de répondre dans les délais auxdits tiers ou autres Responsables de traitement.

4. Sous-traitants ultérieurs

4.1 Le Fournisseur transmettra à Kyndryl un préavis écrit avant d'ajouter un nouveau Sous-traitant ultérieur ou d'élargir le périmètre de Traitement d'un Sous-traitant ultérieur existant. Ledit préavis écrit identifiera le nom du Sous-traitant ultérieur et décrira le périmètre nouveau ou élargi du Traitement. Kyndryl pourra à tout moment s'opposer à l'ajout d'un nouveau Sous-traitant ultérieur ou à l'élargissement du périmètre de Traitement pour des motifs raisonnables et, dans ce cas, les parties travailleront ensemble de bonne foi pour s'adapter à l'opposition de Kyndryl. Sans préjudice du droit de Kyndryl de s'y opposer à tout moment, le Fournisseur est autorisé à faire appel au nouveau Sous-traitant ultérieur ou à élargir le périmètre de Traitement du Sous-traitant ultérieur existant si Kyndryl n'a pas soulevé d'objection dans les 30 Jours suivant la date du préavis écrit du Fournisseur.

4.2 Le Fournisseur imposera les obligations de protection de données, de sécurité et de certification énoncées dans les présentes Conditions à chaque Sous-traitant ultérieur agréé, avant qu'un Sous-traitant Traite des Données de Kyndryl. Le Fournisseur demeure entièrement responsable vis-à-vis de Kyndryl du respect des obligations de chaque Sous-traitant ultérieur.

5. Traitement de données transfrontalier

Définition des termes utilisés ci-dessous :

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.

Importateur de Données signifie Sous-traitant ou Sous-traitant ultérieur non établi dans un Pays adéquat.

Clauses Contractuelles Types de l'UE (« CCT de l'UE ») désigne les Clauses Contractuelles Types de l'UE (Décision de la Commission 2021/914) avec les clauses facultatives appliquées à l'exception de l'option 1 de la Clause 9(a) et de l'option 2 de la Clause 17, telles que publiées officiellement à l'adresse https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Clauses Contractuelles Types serbes (« CCT serbes ») désigne les Clauses Contractuelles Types serbes telles qu'adoptées par le « Commissaire serbe à l'information d'importance publique et à la protection des données personnelles », publiées à l'adresse https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

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 Sous-traitants non établis dans des Pays adéquats.

Annexe du Royaume-Uni relatif au transfert international de données aux clauses contractuelles types de la Commission européenne (« Annexe britannique ») désigne l'annexe du Royaume-Uni relative au transfert international de données aux Clauses contractuelles types de la Commission européenne, tel que publiée officiellement à l'adresse https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

L'annexe suisse aux Clauses contractuelles types de la Commission européenne (« annexe suisse ») désigne les clauses contractuelles applicables aux Clauses contractuelles types de la Commission européenne conformément à la décision de l'Autorité suisse de protection des données (**« PFPDT »**) et à la Loi fédérale suisse sur la protection des données (**« LPD »**).

5.1 Le Fournisseur s'engage à ne pas transférer ou divulguer (y compris au moyen d'un accès à distance) les Données à caractère personnel de Kyndryl au-delà des frontières sans l'accord préalable écrit de Kyndryl. Si

Kyndryl donne cet accord, les parties collaboreront pour veiller au respect des lois applicables sur la protection des données. Si les CCT sont requises par ces lois, le Fournisseur conclura les CCT dans les meilleurs délais sur demande de Kyndryl.

5.2 Concernant les CCT de l'UE :

(a) Si le Fournisseur n'est pas établi dans un Pays adéquat : le Fournisseur conclut par les présentes des CCT de l'UE en tant qu'Importateur de Données avec Kyndryl, et le Fournisseur conclura des accords écrits avec chaque Sous-traitant ultérieur approuvé, conformément à la Clause 9 des CCT de l'UE, et fournira une copie de ces accords à Kyndryl sur demande.

(i) Le Module 1 des CCT de l'UE ne s'applique pas, sauf accord écrit contraire des parties.

(ii) Le Module 2 des CCT de l'UE s'applique lorsque Kyndryl est un Responsable du traitement, et le Module 3 s'applique lorsque Kyndryl est un Sous-traitant. Conformément à la Clause 13 des CCT de l'UE, lorsque les Modules 2 ou 3 s'appliquent, les parties conviennent que (1) les CCT de l'UE seront régies par la loi de l'État membre de l'UE où se trouve l'autorité de supervision compétente et (2) tout litige découlant des CCT de l'UE sera porté devant les tribunaux de l'état membre de l'UE où se trouve l'autorité de supervision compétente. Si la loi mentionnée en 1) ne permet pas aux tiers de bénéficier des droits, les CCT de l'UE seront régies par la loi des Pays-Bas et tout litige découlant des CCT de l'UE mentionné au point 2) sera résolu par le tribunal d'Amsterdam aux Pays-Bas.

(b) Si les deux parties, le Fournisseur et Kyndryl, sont établies dans un Pays adéquat, le Fournisseur agira en tant qu'Exportateur de Données et conclura des CCT de l'UE avec chaque Sous-traitant ultérieur approuvé d'un Pays non adéquat. Le Fournisseur effectuera l'évaluation de l'impact du transfert (TIA) requise et notifiera à Kyndryl sans délai indu (1) toute nécessité d'appliquer des mesures supplémentaires et (2) les mesures appliquées. Sur demande, le Fournisseur fournira à Kyndryl les résultats de la TIA et toute information nécessaire à leur compréhension et leur évaluation. Dans le cas où Kyndryl ne serait pas d'accord avec les résultats de la TIA du Fournisseur ou les mesures supplémentaires appliquées, Kyndryl et le Fournisseur travailleront ensemble à trouver une solution réalisable. Kyndryl se réserve le droit de suspendre ou de mettre fin aux services du Fournisseur concernés sans indemnisation. Pour éviter toute ambiguïté, cela ne dispense pas les Sous-traitants ultérieurs du Fournisseur de l'obligation de devenir partie aux CCT de l'UE avec Kyndryl ou ses Clients comme indiqué dans la section 5.2 (d) ci-dessous.

(c) Si le Fournisseur est établi dans l'Espace économique européen et que Kyndryl est un Responsable de traitement non soumis au Règlement Général sur la Protection des Données 2016/679, le Module 4 des CCT de l'UE s'applique et le Fournisseur conclut par les présentes des CCT de l'UE en tant qu'exportateur de données avec Kyndryl. Si le Module 4 des CCT de l'UE s'applique, les parties conviennent que les CCT de l'UE seront soumises à la loi des Pays-Bas et que tout litige découlant des CCT de l'UE sera résolu par le tribunal d'Amsterdam aux Pays-Bas.

(d) Si d'autres Responsables de traitement, tels que des Clients ou des affiliés, demandent à devenir partie aux CCT de l'UE conformément à la « clause d'ancrage » de la Clause 7, le Fournisseur accepte par les présentes ces demandes.

(e) Les Mesures Techniques et Organisationnelles requises pour se conformer à l'Annexe II des CCT de l'UE se trouvent dans les présentes Conditions, dans le Document de Transaction lui-même et dans le contrat de base associé entre les parties.

(f) En cas de contradiction entre les CCT de l'UE et les présentes Conditions, les CCT de l'UE prévalent.

5.3 S'agissant de la/les annexe(s) britannique(s) :

(a) Si le fournisseur n'est pas établi dans un pays répondant aux conditions requises : (i) le fournisseur conclut par les présentes un ou plusieurs addenda britannique(s) avec Kyndryl en tant qu'importateur afin de compléter les clauses contractuelles types de l'UE énoncées ci-dessus (selon le cas, en fonction des circonstances des activités de traitement) ; et (ii) le fournisseur conclura des accords écrits avec chaque sous-traitant approuvé, et fournira à Kyndryl des copies desdits accords sur demande.

(b) Sous réserve que le fournisseur soit établi dans un pays répondant aux conditions requises, et que Kyndryl soit un responsable du traitement non soumis au Règlement général sur la protection des données du Royaume-Uni (tel qu'incorporé au droit britannique en vertu de l'European Union (Withdrawal) Act 2018), le fournisseur conclut par la présente un/des addenda britannique(s) avec Kyndryl en tant qu'exportateur afin de compléter les clauses contractuelles types de l'UE énoncées à l'article 5.2 paragraphe (b) ci-dessus.

(c) Si d'autres contrôleurs de données, tels que des clients ou des sociétés affiliées, demandent à devenir partie à/aux addenda britannique(s), le fournisseur accepte par la présente une demande similaire.

(d) Les informations relatives aux annexes (telles que définies dans le tableau 3) du/des addenda britannique(s) sont disponibles dans les clauses contractuelles types de l'UE applicables, dans les présentes, dans le document transactionnel lui-même, ainsi que dans l'accord de base connexe entre les parties. Ni Kyndryl ni le fournisseur ne peuvent mettre fin à/aux addenda britannique(s) lorsque ce(s) dernier(s) fait/font l'objet d'une modification.

(e) En cas de conflit entre le(s) addenda britannique(s) et les présentes conditions, le(s) addenda britannique(s) prévaudra/prévaudront.

5.4 Concernant les CCT serbes :

(a) Si le Fournisseur n'est pas établi dans un Pays adéquat : (i) le Fournisseur conclut par les présentes les CCT serbes avec Kyndryl au nom du Fournisseur en tant que Sous-traitant ; et (ii) le Fournisseur conclura des contrats écrits avec chaque Sous-traitant ultérieur agréé, conformément à l'Article 8 des CCT serbes, et fournira à Kyndryl, sur demande, des exemplaires de ces contrats.

(b) Si le Fournisseur est établi dans un Pays adéquat, le Fournisseur accepte par les présentes de respecter les CCT serbes avec Kyndryl au nom de chaque Sous-traitant ultérieur situé dans un Pays non adéquat. Si le Fournisseur n'est pas en mesure de le faire pour un tel Sous-traitant ultérieur, le Fournisseur transmettra à Kyndryl les CCT de l'UE signées par ce Sous-traitant ultérieur pour contresignature par Kyndryl avant d'autoriser le Sous-traitant ultérieur à Traiter les Données à caractère personnel de Kyndryl.

(c) Les CCT serbes entre Kyndryl et le Fournisseur serviront soit de CCT serbes entre un Responsable de traitement et un sous-traitant, soit d'accord écrit consécutif entre le « sous-traitant » et le « sous-traitant ultérieur », selon les circonstances. En cas de contradiction entre les CCT serbes et les présentes Conditions, les CCT serbes prévalent.

(d) Les informations requises pour se conformer aux Annexes 1 à 8 des CCT serbes aux fins de régir le transfert de Données à caractère personnel vers un Pays non adéquat se trouvent dans les présentes Conditions et dans l'Annexe au Document de Transaction, ou dans le Document de Transaction lui-même.

5.5. S'agissant du/des addenda suisse(s) :

(a) Si et dans la mesure où un transfert de Données personnelles de Kyndryl en vertu de la section 5.1. est soumis à la Loi fédérale suisse sur la protection des données (« LPD »), les clauses contractuelles types de l'UE convenues à la section 5.2. des présentes Conditions régissent le transfert, avec les modifications suivantes pour

adopter la norme RGPD pour les Données personnelles suisses :

- Les références au Règlement général sur la protection des données (« RGPD ») s'entendent également comme des références aux dispositions équivalentes de la LPD,
- le PFPDT est l'autorité de contrôle compétente conformément à la clause 13 et à l'annexe I.C des clauses contractuelles types de l'UE
- Le droit suisse comme droit applicable dans le cas où le transfert est exclusivement soumis à la LPD et
- Le terme « État membre » figurant à la clause 18 de la clause contractuelle type de l'UE est étendu à la Suisse afin de permettre aux personnes suisses concernées de faire valoir leurs droits dans leur lieu de résidence habituel.

(b) Pour éviter toute ambiguïté, aucun des éléments ci-dessus ne vise à diminuer le niveau de protection des données fourni par la clause contractuelle type de l'UE de quelque manière que ce soit, mais uniquement à étendre ce niveau de protection aux personnes suisses concernées. Si cela n'est pas le cas et dans la mesure où cela ne l'est pas, la clause contractuelle type de l'UE prévaudra.

6. Assistance et enregistrements

6.1 Compte tenu de la nature du Traitement, le Fournisseur aidera Kyndryl en prenant des mesures techniques et organisationnelles appropriées 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'une Violation 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.

6.2 Le Fournisseur s'engage à conserver un registre à jour du nom et des coordonnées de chaque Sous-traitant ultérieur, notamment de chaque représentant et délégué à la protection des données de chaque Sous-traitant ultérieur. 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.

Article IV, Mesures Techniques et Organisationnelles, Sécurité du Code

Cet Article s'applique si le Fournisseur a accès au Code source de Kyndryl. Le Fournisseur doit respecter les obligations du présent Article et ainsi protéger le Code source de Kyndryl contre toute perte, destruction, modification, divulgation accidentelle ou non autorisée, accès accidentel ou non autorisé et toute autre forme illégale de Gestion. Les obligations énoncées dans le présent Article s'appliquent à toutes les applications, plateformes et infrastructures informatiques que le Fournisseur exploite ou gère lors de la fourniture des Livrables et Services et de la Gestion de la Technologie de Kyndryl, y compris tous les développements, tests, hébergements, supports, opérations et environnements de centre de données.

1. Exigences relatives à la Sécurité

Définition des termes utilisés ci-dessous :

Pays prohibé signifie tout pays (a) désigné par le gouvernement des États-Unis comme étant un adversaire étranger en vertu du décret du 15 mai 2019 relatif à la Sécurisation des Technologies de l'Information et de la Communication et de la Chaîne Logistique des Services, (b) répertorié conformément à l'article 1654 de la Loi U.S. National Defense Authorization Act de 2019, ou (c) désigné comme « Pays prohibé » dans le Document de la Transaction.

1.1 Le Fournisseur ne distribuera ou ne mettra sous séquestre aucun Code source de Kyndryl au profit d'un tiers quel qu'il soit.

1.2. Le Fournisseur ne placera aucun Code source de Kyndryl sur des serveurs situés dans un Pays prohibé.Le Fournisseur ne permettra à quiconque, y compris son Personnel, se trouvant ou se rendant dans un Pays prohibé (durant l'intégralité de cette visite), pour quelque raison que ce soit, d'accéder à ou d'utiliser un Code source de Kyndryl, quel que soit l'emplacement de ce Code source de Kyndryl dans le monde, et le Fournisseur n'autorisera aucun développement, test ou autre prestation nécessitant un tel accès ou une telle utilisation dans un Pays Prohibé.

1.3 Le Fournisseur ne placera ou ne distribuera le Code source de Kyndryl dans aucune juridiction dont la législation ou l'interprétation de la législation exige la divulgation du Code source à un tiers. Si un changement de législation ou d'interprétation de législation dans une juridiction où se situe le Code source de Kyndryl impose au Fournisseur la divulgation dudit Code source à un tiers, le Fournisseur s'engage à détruire ou retirer immédiatement ce Code source de Kyndryl de ladite juridiction et à ne placer aucun autre Code source de Kyndryl dans cette juridiction si ladite législation ou interprétation de la législation demeure en vigueur.

1.4 Le Fournisseur ne devra pas, directement ou indirectement, prendre une mesure, notamment la conclusion d'un ou plusieurs contrats, qui conduirait le Fournisseur, Kyndryl ou un tiers à subir une obligation de divulgation au titre des articles 1654 ou 1655 de la Loi U.S. National Defense Authorization Act de 2019. Par souci de clarté, sauf autorisation expresse dans le Document de Transaction ou dans le contrat de base associé entre les parties, le Fournisseur n'est autorisé à divulguer le Code source de Kyndryl à aucun tiers, en aucune circonstance, sans l'accord préalable écrit de Kyndryl.

1.5 Si Kyndryl notifie au Fournisseur ou si un tiers notifie à l'une des parties que : (a) le Fournisseur a autorisé l'introduction du Code source de Kyndryl dans un Pays prohibé ou dans toute juridiction assujettie à l'alinéa 1.3 ci-dessus ; (b) le Fournisseur a diffusé, consulté ou utilisé le Code source de Kyndryl d'une manière non autorisée par le Document de Transaction ou le contrat de base associé ou tout autre accord entre les parties ou (c) le Fournisseur est en violation avec l'alinéa 1.4 ci-dessus. Alors, et sans limiter les droits dont dispose Kyndryl pour remédier à ce non-respect en vertu de la législation ou des règles d'équité ou au titre du Document de Transaction ou du contrat de base associé ou de tout autre accord entre les parties : (i) si ladite notification est destinée au Fournisseur, ce dernier partagera la notification avec Kyndryl dans les meilleurs délais ; et (ii) le Fournisseur, selon les instructions raisonnables de Kyndryl, étudiera et remédiera au problème dans un délai raisonnablement déterminé par Kyndryl (après consultation du Fournisseur).

1.6 Si Kyndryl estime raisonnablement que des changements de stratégies, procédures, contrôles ou pratiques du Fournisseur en ce qui concerne l'accès au Code source sont nécessaires pour traiter les risques en matière de Sécurité, d'infraction aux droits de propriété intellectuelle ou de risques similaires ou associés

(notamment le risque que, sans ces changements, Kyndryl ne soit pas autorisée à vendre à certains Clients ou sur certains marchés ou ne soit pas en mesure de satisfaire les exigences du Client en matière de Sécurité ou de chaîne logistique), alors Kyndryl pourra contacter le Fournisseur pour discuter des mesures nécessaires permettant de répondre à ces risques, y compris des modifications à apporter à ces stratégies, procédures, contrôles ou pratiques. Sur demande de Kyndryl, le Fournisseur collaborera avec Kyndryl pour évaluer si de telles modifications sont nécessaires et pour mettre en œuvre les modifications appropriées convenues d'un commun accord.

Article V, Développement Sécurisé

Cet Article s'applique si le Fournisseur fournira du Code source ou du Logiciel sur Site lui appartenant ou appartenant à des tiers à Kyndryl, ou si des Livrables ou Services du Fournisseur seront fournis à un Client de Kyndryl dans le cadre d'un produit ou service de Kyndryl.

1. État de préparation de la sécurité

1.1 Le Fournisseur participera aux processus internes de Kyndryl qui évaluent le niveau de sécurité des produits et services de Kyndryl qui reposent sur l'un des Livrables du Fournisseur, notamment en répondant dans les délais et en intégralité aux demandes d'informations, que ce soit par le biais de documents, d'autres registres, d'entretiens avec le Personnel concerné du Fournisseur, etc.

2. Sécurité du développement

2.1 Cette Section 2 s'applique uniquement lorsque le Fournisseur fournit des Logiciels sur Site à Kyndryl.

2.2 Le Fournisseur a mis en œuvre et maintiendra pendant toute la durée du Document de Transaction, conformément aux Bonnes pratiques du secteur, le réseau, la plateforme, le système, l'application, le périphérique, l'infrastructure physique, la réponse aux incidents et les politiques, procédures et contrôles de sécurité axées sur le Personnel qui sont nécessaires pour protéger : (a) les systèmes et environnements de développement, de construction, de test et d'exploitation que le Fournisseur ou tout tiers engagé par le Fournisseur exploite, gère, utilise ou sur lesquels il s'appuie pour ou concernant les Livrables et (b) tout le code source des Livrables contre la perte, les formes illicites de manipulation, et l'accès, la divulgation ou la modification non autorisés.

3. Certification ISO 20243

3.1 Cette section 3 ne s'applique que si un ou des Livrables ou Services du Fournisseur seront fournis à un Client de Kyndryl dans le cadre d'un produit ou service de Kyndryl.

3.2 Le Fournisseur devra obtenir une certification de conformité à la norme ISO 20243, Technologies de l'Information - Norme de Fournisseur de Technologie de Confiance Ouverte (O-TTPS), Atténuation des produits contrefaits et malicieusement contaminés (soit une certification par auto-évaluation, soit une certification basée sur l'évaluation d'un auditeur indépendant réputé). Alternativement, sous réserve de la demande écrite du Fournisseur et de l'accord écrit de Kyndryl, le Fournisseur obtiendra une certification de conformité à une norme substantiellement équivalente applicable en matière de développement sécurisé et de pratiques de gestion de la chaîne logistique (soit une certification par auto-évaluation, soit une certification basée sur l'évaluation d'un auditeur indépendant réputé, si et dans la mesure où Kyndryl donne son accord).

3.3 Le Fournisseur obtiendra la certification de conformité à la norme ISO 20243 ou à une norme du secteur sensiblement équivalente (si Kyndryl l'approuve par écrit) dans les 180 jours suivant la date d'effet du Document de Transaction
puis renouvellera la certification tous les 12 mois par la suite (chaque renouvellement se faisant par rapport à la version alors la plus récente de la norme applicable, à savoir la norme ISO 20243 ou, si approuvé par écrit par

Kyndryl, une norme de l'industrie sensiblement équivalente couvrant les pratiques sécurisées de développement et de chaîne d'approvisionnement).

3.4 Le Fournisseur transmettra à Kyndryl, sur demande, un exemplaire des certifications que le Fournisseur est tenu de se procurer, conformément aux alinéas 2.1 et 2.2 ci-dessus.

4. Vulnérabilités en matière de Sécurité

Définition des termes utilisés ci-dessous :

Rectification d'Erreur désigne les correctifs de bogues et révisions visant à corriger des erreurs ou des déficiences, y compris des Vulnérabilités en matière de Sécurité, relevés dans les Livrables.

Atténuation désigne tout moyen connu permettant d'atténuer ou d'éviter les risques d'une Vulnérabilité en matière de Sécurité.

Vulnérabilité en matière de Sécurité désigne un état de la conception, du codage, du développement, de l'implémentation, des tests, des opérations, de l'assistance, de la maintenance ou de la gestion d'un Livrable qui permet une attaque par quiconque et qui pourrait donner lieu à un accès ou une exploitation non autorisée, notamment : (a) l'accès, le contrôle ou l'interruption du fonctionnement d'un système, (b) l'accès à des données, leur suppression, leur modification ou leur extraction ou (c) des modifications de l'identité, des autorisations ou des droits d'accès des utilisateurs ou administrateurs. Une Vulnérabilité en matière de Sécurité peut exister indépendamment du fait qu'un identifiant CVE (Common Vulnerabilities or Exposures) ou toute évaluation ou classification officielle lui soit attribuée ou non.

4.1 Le Fournisseur se porte garant et s'engage à : (a) mettre en œuvre les Bonnes pratiques du secteur visant à identifier des Vulnérabilités en matière de Sécurité, y compris au moyen d'analyses de sécurité portant sur l'application du code source statique et dynamique, d'analyses de sécurité open-source et d'analyses des vulnérabilités du système, et (b) se conformer aux présentes Conditions afin de prévenir, détecter et corriger les Vulnérabilités en matière de Sécurité relevées dans les Livrables et dans toutes les applications, plateformes et infrastructures informatiques par le biais desquelles le Fournisseur procède à la création et à la livraison des Services et Livrables.

4.2 Si le Fournisseur relève une Vulnérabilité en matière de Sécurité affectant l'un de ses Livrables ou l'une des applications, plateformes ou infrastructures informatiques, il procurera à Kyndryl un Correctif et des mesures d'Atténuation pour toutes les versions et éditions des Livrables, conformément aux Niveaux de gravité et aux délais définis dans les tableaux ci-dessous :

Niveau de Gravité*
Urgence : Vulnérabilité en matière de Sécurité constituant une menace grave et potentiellement mondiale. Kyndryl désigne les Vulnérabilités en matière de Sécurité d'Urgence à son entière discrétion, quel que soit le Score de base CVSS.
Critique : Vulnérabilité en matière de Sécurité dont le Score de base CVSS est compris entre 9 et 10,0
Élevée : Vulnérabilité en matière de Sécurité dont le Score de base CVSS est compris entre 7,0 et 8,9
Moyenne : Vulnérabilité en matière de Sécurité dont le Score de base CVSS est compris entre 4,0 et 6,9
Faible : Vulnérabilité en matière de Sécurité dont le Score de base CVSS est compris entre 0,0 et 3,9

Délais				
Urgence	***Critique***	***Elevée***	***Moyen***	***Faible***
4 Jours ou moins, comme déterminé par le Directeur de la sécurité des systèmes d'information de Kyndryl	30 Jours	30 Jours	90 Jours	Conformément aux Bonnes pratiques du secteur

* Lorsque le Score de base CVSS n'a pas été défini pour une Vulnérabilité de Sécurité, le Fournisseur appliquera un niveau de gravité adapté à la nature et aux circonstances de ladite vulnérabilité.

4.3 Pour une Vulnérabilité en matière de sécurité qui a été communiquée publiquement et pour laquelle le Fournisseur n'a pas encore fourni de Correctif ou d'Atténuation à Kyndryl, le Fournisseur mettra en œuvre autant de contrôles supplémentaires de sécurité que possible visant à atténuer les risques liés à la vulnérabilité.

4.4 Si Kyndryl n'est pas satisfaite de la réponse du Fournisseur à une Vulnérabilité en matière de Sécurité d'un Livrable ou de toute application, plateforme ou infrastructure susmentionnée, sans préjudice de tout autre droit de Kyndryl, le Fournisseur prendra rapidement les mesures nécessaires permettant à Kyndryl de discuter de ses préoccupations directement avec un Vice-Président ou un dirigeant équivalent responsable de la livraison du Correctif.

4.5 Les exemples de Vulnérabilités en matière de Sécurité comprennent le code tiers ou code open-source en fin de service (end-of-service, EOS) lorsque ces types de code ne bénéficient plus de correctifs de sécurité.

Article VI, Accès aux Systèmes d'Entreprise

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

1. Conditions Générales

1.1 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 demander à ses employés disposant dudit accès de se conformer aux exigences du présent Article.

1.2 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.

1.3 Les employés du Fournisseur sont autorisés uniquement à accéder aux Systèmes d'Entreprise et pourront uniquement utiliser les Périphériques pour lesquels Kyndryl autorise cet accès afin de fournir les Services. Les employés du Fournisseur ne pourront pas utiliser les Périphériques ainsi autorisés par 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.

1.4 Par souci de clarté, les employés du Fournisseur s'engagent à ne pas utiliser les Périphériques ainsi autorisés par Kyndryl pour accéder aux Systèmes d'Entreprise pour des raisons personnelles (par exemple, les employés du Fournisseur ne sont pas autorisés à stocker des fichiers personnels tels que musique, vidéos, images ou autres éléments similaires sur lesdits Périphériques et ne peuvent pas utiliser l'Internet à partir de ces Périphériques pour des raisons personnelles).

1.5 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).

1.6 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.

1.7 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 : (a) n'est plus employé par le Fournisseur, (b) 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.

1.8 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.

1.9 Le Fournisseur ne doit autoriser aucun employé d'une 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.

2. Logiciel de Périphérique

2.1 Le Fournisseur demandera à ses employés d'installer rapidement tous les logiciels de Périphérique nécessaires pour permettre à Kyndryl d'assurer l'accès sécurisé aux Systèmes d'Entreprise. Ni le Fournisseur, ni ses employés n'interféreront dans les opérations de ce logiciel ou les dispositifs de sécurité activés par le logiciel.

2.2 Le Fournisseur et ses employés respecteront les règles de configuration de Périphérique définies par Kyndryl et collaboreront avec Kyndryl pour garantir le fonctionnement du logiciel de la manière prévue par Kyndryl. Par exemple, le Fournisseur n'est pas autorisé à contourner les fonctions de blocage de site Web ou d'application automatisée de correctifs.

2.3 Les employés du Fournisseur ne sont pas autorisés à partager avec toute autre personne les Périphériques qu'ils utilisent pour accéder aux Systèmes d'Entreprise, ni leurs noms d'utilisateur, mots de passe, etc. associés aux Périphériques.

2.4 Si Kyndryl autorise les employés 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.

3. Supervision et Coopération

3.1 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 (a) mener un test de sécurité sur n'importe quel Périphérique, (b) 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 (c) 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).

3.2 Kyndryl pourra à tout moment révoquer l'accès physique aux Systèmes d'Entreprise pour tout ou partie des employés 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.

3.3 Les droits de Kyndryl ne sont bloqués, diminués ou restreints en aucune façon par aucune condition du Document de Transaction, du contrat de base associé entre les parties ou de tout autre accord entre les parties, notamment aucune condition pouvant exiger que des données, éléments ou autres informations de quelque nature que ce soit soient exclusivement conservées sur un ou plusieurs sites sélectionnés ou que seules les personnes d'un ou plusieurs sites sélectionnés puissent accéder à ces données, éléments ou autres informations.

4. Périphériques de Kyndryl

4.1 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 d'altération désignant toute modification d'un Périphérique, y compris des logiciels, applications, conceptions de sécurité, configurations de paramètres de sécurité ou de la conception physique, mécanique ou électrique d'un Périphérique.

4.2 Le Fournisseur restituera tous les Périphériques de Kyndryl dans les cinq (5) jours ouvrables après que ces Périphériques ne soient 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 Bonnes pratiques du secteur relatives à la suppression définitive de tous ces éléments, données ou autres informations. Le Fournisseur devra, à ses frais, conditionner les Périphériques 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 alinéa 4.2 constitue une violation substantielle du Document de Transaction et du contrat 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 ce contrat.

4.3 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.

4.4. 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.

5. Mises à Jour

5.1 Nonobstant toute disposition contraire dans le Document de Transaction ou le contrat de base associé entre les parties, Kyndryl pourra, sans notification écrite au Fournisseur et sans avoir besoin de l'accord du Fournisseur, mettre à jour, compléter ou modifier le présent Article pour satisfaire à toute exigence d'une loi applicable ou une obligation du Client, afin de prendre en considération l'éventuelle évolution des Bonnes pratiques en matière de sécurité ou toute autre exigence jugée nécessaire par Kyndryl pour protéger Kyndryl ou les Systèmes d'entreprise.

Article VII, Renforcement du Personnel

Le présent Article s'applique si les employés du Fournisseur vont consacrer la totalité de leur temps de travail à fournir des Services pour Kyndryl, à réaliser tous ces Services dans les locaux de Kyndryl, les locaux du Client ou à partir de leur domicile et à fournir les Services uniquement en utilisant les Périphériques de Kyndryl pour accéder aux Systèmes d'Entreprise.

1. Accès aux Systèmes d'Entreprise : Environnements de Kyndryl

1.1 Le Fournisseur n'est autorisé à fournir les Services qu'en accédant aux Systèmes d'Entreprise à l'aide des Périphériques fournis par Kyndryl.

1.2 Le Fournisseur respectera les conditions de l'Article VI (Accès aux Systèmes d'Entreprise) pour tous les accès aux Systèmes d'Entreprise.

1.3 Les Périphériques fournis par Kyndryl sont les seuls Périphériques que le Fournisseur et ses employés sont autorisés à utiliser pour fournir les Services et ne peuvent être utilisés par le Fournisseur et ses employés que pour fournir les Services. Par souci de clarté, le Fournisseur ou ses employés ne sont en aucun cas autorisés à utiliser d'autres périphériques pour fournir les Services ou à utiliser les Périphériques de Kyndryl pour tout autre client du Fournisseur ou à des fins autres que la fourniture des Services à Kyndryl.

1.4 Les employés du Fournisseur utilisant les Périphériques de Kyndryl peuvent partager, les uns avec les autres, les Éléments de Kyndryl et stocker ces derniers sur les Périphériques de Kyndryl, mais uniquement dans les limites de partage et stockage nécessaires pour la réalisation en bonne et due forme des Services.

1.5 Sauf en ce qui concerne un tel stockage sur les Périphériques de Kyndryl, le Fournisseur ou ses employés ne sont en aucun cas autorisés à retirer les Éléments de Kyndryl des référentiels, environnements, outils ou infrastructures de Kyndryl dans lesquels ils sont conservés par Kyndryl.

1.6 Par souci de clarté, le Fournisseur et ses employés ne sont autorisés à transférer les Éléments de Kyndryl vers aucun référentiel, environnement, outil ou infrastructure du Fournisseur ou vers aucun autre système, plateforme, réseau, etc. du Fournisseur, sans l'accord préalable écrit de Kyndryl.

1.7 L'Article VIII (Mesures Techniques et Organisationnelles, Sécurité Générale) ne s'applique pas aux Services du Fournisseur si les employés du Fournisseur vont consacrer la totalité de leur temps de travail à la fourniture de Services pour Kyndryl, réaliser tous ces Services dans les locaux de Kyndryl, les locaux du Client ou à partir de leur domicile et fournir les Services uniquement en utilisant des Périphériques de Kyndryl pour accéder aux Systèmes d'Entreprise. Dans le cas contraire, l'Article VIII s'applique aux Services du Fournisseur.

Article VIII, Mesures Techniques et Organisationnelles, Sécurité des Données

Cet Article s'applique si le Fournisseur fournit des Services ou des Livrables à Kyndryl, sauf si le Fournisseur aura uniquement accès aux BCI de Kyndryl lors de la fourniture de ces Services et Livrables (c'est-à-dire que le Fournisseur ne Traitera aucune autre Donnée de Kyndryl et n'aura accès à aucun autre Élément de Kyndryl ni à aucun Système d'Entreprise), si les seuls Services et Livrables du Fournisseur consistent à fournir des Logiciels sur Site à Kyndryl, ou si le Fournisseur fournit tous ses Services et Livrables selon un modèle d'extension du personnel conformément à l'Article VII, y compris la Section 1.7 de celui-ci.

Le Fournisseur doit respecter les obligations du présent Article et ainsi protéger : (a) les Éléments de Kyndryl contre toute perte, destruction, modification, divulgation accidentelle ou non autorisée, accès accidentel ou non autorisé, (b) les Données de Kyndryl contre toute autre forme illégale de Traitement et (c) la Technologie de Kyndryl contre toute forme illégale de Gestion. Les obligations énoncées dans le présent Article s'appliquent à toutes les applications, plateformes et infrastructures informatiques que le Fournisseur exploite ou gère lors de la fourniture des Livrables et Services et de la Gestion de la Technologie de Kyndryl, y compris tous les développements, tests, hébergements, supports, opérations et environnements de centre de données.

1. Politiques de Sécurité

1.1 Le Fournisseur mettra en place et respectera les politiques et pratiques en matière de Sécurité informatique nécessaires aux activités du Fournisseur, qui seront obligatoires pour tout le Personnel du Fournisseur et qui sont conformes aux Bonnes pratiques du secteur.

1.2 Le Fournisseur évaluera ses politiques et pratiques de sécurité informatique au moins une fois par an et les modifiera si le Fournisseur le juge nécessaire pour protéger les Éléments de Kyndryl.

1.3 Le Fournisseur gérera et respectera ses obligations d'attestation d'emploi standard pour tous les nouveaux employés et appliquera lesdites obligations à tout son Personnel et à ses filiales détenues à 100 %. 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 périodiquement ces obligations, s'il le juge nécessaire.

1.4 Le Fournisseur dispensera annuellement à ses employés une formation dans les domaines de la sécurité et de la confidentialité et demandera à tous ces employés de certifier chaque année qu'ils respecteront les politiques du Fournisseur en matière d'éthique professionnelle, de Confidentialité et de Sécurité, telles qu'elles sont exposées dans le code de conduite ou des documents similaires du Fournisseur. Le Fournisseur dispensera aux personnes ayant un accès administrateur aux Services, Livrables et Éléments de Kyndryl une formation supplémentaire sur les politiques et processus spécifiques à leur rôle et à la prise en charge des Services, Livrables et Éléments de Kyndryl, et en fonction des besoins pour maintenir la conformité et les certifications nécessaires.

1.5 Le Fournisseur doit concevoir des mesures de sécurité et de confidentialité afin de protéger et d'assurer la disponibilité des Éléments de Kyndryl, notamment par la mise en œuvre, la tenue à jour et le respect des politiques et procédures qui exigent la sécurité et la confidentialité dès la conception (« Security and Privacy by design »), la sécurité de l'ingénierie et la sécurité des opérations, pour tous les Services et Livrables et pour toutes les Gestions de la Technologie de Kyndryl.

2. Incidents de Sécurité

2.1 Le Fournisseur mettra en place et respectera les politiques de résolution d'incident documentée, conformément aux Bonnes pratiques du secteur relatives au traitement des incidents de sécurité informatique.

2.2 Le Fournisseur enquêtera sur les accès non autorisés ou l'utilisation non autorisée des Éléments de Kyndryl et définira et exécutera un plan d'intervention approprié.

2.3 Le Fournisseur s'engage à notifier à Kyndryl dans les meilleurs délais (et au plus tard dans les 48 heures) après avoir pris connaissance de toute Violation de Sécurité. Le Fournisseur enverra cette notification à l'adresse cyber.incidents@kyndryl.com. Le Fournisseur fournira à Kyndryl toute information raisonnablement demandée sur cette violation et sur le statut de toute activité de résolution et de restauration du Fournisseur. À titre d'exemple, les informations raisonnablement demandées peuvent inclure des historiques démontrant un accès privilégié, administratif et autre aux appareils, aux systèmes ou aux

applications, des images d'appareils, de systèmes ou d'applications, et d'autres éléments similaires, dans la mesure pertinente à la résolution de la violation ou des activités de réparation ou de restauration du Fournisseur.

2.4 Le Fournisseur fournira à Kyndryl une assistance raisonnable pour satisfaire à toutes les obligations légales (y compris les obligations de notification aux régulateurs ou aux Personnes Concernées) de Kyndryl, des sociétés affiliées et Clients de Kyndryl (et de leurs clients et sociétés affiliées) en relation avec une Violation de Sécurité.

2.5 Le Fournisseur n'informera ni ne signalera à aucun tiers qu'une Violation de Sécurité est directement ou indirectement liée à Kyndryl ou aux Éléments de Kyndryl, sauf si Kyndryl l'approuve par écrit ou lorsque la loi l'exige. Le Fournisseur avertira Kyndryl par écrit avant de distribuer toute notification requise par la loi à un tiers, si la notification est de nature à révéler directement ou indirectement l'identité de Kyndryl.

2.6 Dans le cas d'une Violation de Sécurité découlant du manquement du Fournisseur à une obligation au titre des présentes Conditions :

(a) le Fournisseur prendra en charge tous les coûts qu'il engage ainsi que les frais réels encourus par Kyndryl pour l'envoi d'une notification de Violation de Sécurité aux autorités compétentes concernées ou à tout autre organisme gouvernemental ou instance d'autorégulation du secteur d'activité concerné, aux médias (si la loi applicable l'exige), ainsi qu'aux Personnes Concernées, Clients et autres ;

(b) à la demande de Kyndryl, le Fournisseur mettra en place et maintiendra, à ses propres frais, un centre d'appels pour répondre aux questions des Personnes Concernées sur la Violation de Sécurité et ses conséquences, pendant le délai garantissant la meilleure protection, à savoir soit une période d'un an suivant la date à laquelle la Violation de Sécurité a été notifiée auxdites Personnes Concernées, soit conformément aux exigences de la loi applicable sur la protection des données. Kyndryl et le Fournisseur collaboreront pour créer les scripts et autres éléments à utiliser par le personnel du centre d'appels lorsqu'il répond aux demandes. Alternativement, moyennant un préavis écrit adressé au Fournisseur, Kyndryl pourra mettre en place et gérer son propre centre d'appels au lieu de demander au Fournisseur de mettre en place un centre d'appels, et le Fournisseur remboursera à Kyndryl les coûts réels engagés par Kyndryl lors de la mise en place et de la gestion dudit centre d'appels ; et

(c) le Fournisseur remboursera à Kyndryl les coûts réels de prestation de services de suivi de crédit et de rétablissement de crédit engagés par Kyndryl, pendant le délai garantissant la meilleure protection, à savoir soit une période d'un an suivant la date de notification de la Violation de Sécurité à tous les individus concernés par la violation qui choisissent de souscrire à ces services, soit conformément aux exigences d'une loi applicable sur la protection des données.

3. Contrôle de sécurité et d'Entrée Physique (le terme « Installation », tel qu'il est utilisé ci-dessous, signifie un emplacement physique dans lequel le Fournisseur héberge ou traite les Éléments de Kyndryl ou y accède).

3.1 Le Fournisseur mettra en place les dispositifs de contrôle d'Entrée Physique appropriés, tels que des barrières, des points d'entrée contrôlés par carte, des caméras de surveillance et des bureaux de réception surveillés, afin d'empêcher toute entrée non autorisée dans les Installations.

3.2 Le Fournisseur exigera une autorisation d'accès aux Installations et aux zones contrôlées des Installations, y compris tout accès temporaire, et limitera les accès par rôle professionnel et en fonction des besoins professionnels. Si le Fournisseur accorde un accès temporaire, son employé habilité accompagnera tout visiteur se trouvant dans l'Installation et dans les zones contrôlées.

3.3 Le Fournisseur mettra en place des contrôles d'accès, y compris les contrôles d'accès multi-facteur conformes aux Bonnes pratiques du secteur, afin de restreindre de manière appropriée l'entrée dans les zones contrôlées des Installations, consignera dans des journaux toutes les tentatives d'entrée et conservera ces journaux pendant au moins un an.

3.4 Le Fournisseur révoquera l'accès aux Installations et aux zones contrôlées des Installations (a) dès la rupture du contrat de travail d'un employé habilité du Fournisseur ou (b) lorsque l'employé habilité du Fournisseur n'a plus de motif professionnel valable pour y accéder. Le Fournisseur se conformera aux

procédures formelles de rupture de contrat de travail qui comprennent le retrait de l'employé, dans les plus brefs délais, des listes de contrôle d'accès et la restitution des badges d'accès physique.

3.5 Le Fournisseur prendra les précautions nécessaires pour protéger toutes les infrastructures physiques utilisées à l'appui des Services et Livrables et de la Gestion de la Technologie de Kyndryl contre les menaces environnementales, tant d'origine naturelle qu'humaine, par exemple température ambiante excessive, incendie, inondation, humidité, vol et vandalisme.

4. Contrôle d'accès, d'intervention, de transfert et de séparation

4.1 Le Fournisseur maintiendra l'architecture de sécurité documentée des réseaux qu'il gère lorsqu'il utilise les Services, fournit des Livrables et Gère la Technologie de Kyndryl. Le Fournisseur passera en revue séparément ladite architecture de réseau et prendra les mesures permettant d'empêcher les connexions réseau non autorisées aux systèmes, applications et périphériques réseau, afin de garantie la conformité aux normes en matière de segmentation sécurisée, d'isolement et de protection complète. Le Fournisseur n'est pas autorisé à utiliser la technologie sans fil dans le cadre de l'hébergement et des opérations des Services Hébergés ; cependant, le Fournisseur peut utiliser la technologie réseau sans fil pour la livraison des Services et Livrables et pour la Gestion de la Technologie de Kyndryl, mais il devra appliquer un chiffrement et exiger une authentification sécurisée pour ces réseaux sans fil.

4.2 Le Fournisseur mettra en place des mesures destinées à séparer logiquement les Éléments de Kyndryl et à empêcher que ces derniers soient exposés ou accessibles aux personnes non autorisées. En outre, le Fournisseur mettra en place une isolation appropriée de ses environnements de production et hors production et de 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 en termes de sécurité et de protection de données dans l'environnement hors production soient équivalentes à celles de l'environnement de production.

4.3 Le Fournisseur chiffrera les Éléments de Kyndryl en transit et stockés (sauf si le Fournisseur démontre, à la satisfaction raisonnable de Kyndryl, que le chiffrement des Éléments de Kyndryl stockés est techniquement irréalisable). Le Fournisseur chiffrera également tous les supports physiques, le cas échéant, tels que les supports contenant des fichiers de sauvegarde. Le Fournisseur gérera des procédures documentées pour la génération, l'émission, la distribution, le stockage, la rotation, la révocation, la restauration, la sauvegarde, la destruction, l'accès et l'utilisation sécurisés des clés en association avec le chiffrement de données. Le Fournisseur veillera à ce que les méthodes cryptographiques spécifiques utilisées pour ces chiffrements soient conformes aux Bonnes pratiques du secteur (telles que NIST SP 800-131a).

4.4 Si le Fournisseur requiert l'accès à des Éléments de Kyndryl, le Fournisseur restreindra et limitera cet accès au niveau minimum requis pour la fourniture et le support des Services et Livrables. Le Fournisseur exigera que ledit accès, y compris l'accès administrateur aux composants sous-jacents (c'est-à-dire l'accès privilégié) soit individuel, basé sur les rôles et soumis à l'accord et la validation régulière des employés habilités du Fournisseur conformément aux principes de séparation des tâches. Le Fournisseur mettra en place des mesures permettant d'identifier et de supprimer les comptes redondants et inactifs. Le Fournisseur révoquera également les comptes dotés d'un accès privilégié, dans les vingt-quatre (24) heures suivant la rupture du contrat de travail du détenteur du compte ou la demande de Kyndryl ou des employés habilités du Fournisseur, par exemple le responsable du détenteur de compte.

4.5 Conformément aux Bonnes pratiques du secteur, le Fournisseur mettra en place des mesures techniques imposant un délai d'expiration pour les sessions inactives, le verrouillage des comptes après plusieurs échecs de tentative de connexion successifs, l'authentification à l'aide d'un mot de passe ou d'une phrase passe fiable, ainsi que des mesures nécessitant le transfert et le stockage sécurisés desdits mots de passe et phrases passe. En outre, le Fournisseur utilisera l'authentification multi-facteur pour tous les accès privilégiés hors console aux Éléments de Kyndryl.

4.6 Le Fournisseur surveillera l'utilisation des accès privilégiés et tiendra à jour les informations de sécurité et les mesures de gestion d'événement destinées : (a) à identifier les accès et activités non autorisés, (b) à permettre une réponse rapide et appropriée auxdits accès et activités et (c) à permettre des audits par le Fournisseur, Kyndryl (conformément à ses droits de vérification définis dans les présentes Conditions et à ses

droits d'audit définis dans le Document de Transaction ou le contrat de base associé ou tout autre accord connexe entre les parties) et des tiers de la conformité aux politiques documentées du Fournisseur.

4.7 Le Fournisseur conservera des journaux dans lesquels il enregistrera, conformément aux Bonnes pratiques du secteur, tous les accès ou activités administrateur, utilisateur ou autres relatifs aux systèmes utilisés dans le cadre de la fourniture de Services ou Livrables et de la Gestion de la Technologie de Kyndryl (et fournira ces journaux à Kyndryl sur demande). Le Fournisseur mettra en place des mesures de protection contre l'accès non autorisé, la modification et la destruction accidentelle ou délibérée desdits journaux.

4.8 Le Fournisseur gérera des dispositifs de protection informatique pour les systèmes dont il est propriétaire ou qu'il gère, y compris les systèmes d'utilisateur final, et qu'il utilise dans le cadre de la fourniture de Services ou Livrables ou de la Gestion de la Technologie de Kyndryl, comprenant notamment des pare-feux terminaux, le chiffrement de disque complet, les technologies de détection de terminaux et d'intervention basées sur la signature et la non-signature pour éliminer les programmes malveillants et les menaces persistantes sophistiquées, les verrouillages d'écran temporels et les solutions de gestion de terminaux imposant des obligations d'application de correctif et de configuration des paramètres de sécurité. En outre, le Fournisseur mettra en place des dispositifs de contrôles techniques et opérationnels pour s'assurer que seuls les systèmes des utilisateurs finaux connus et sécurisés sont autorisés à utiliser les réseaux du Fournisseur.

4.9 Conformément aux Bonnes pratiques du secteur, le Fournisseur mettra en place des dispositifs de protection pour les environnements de centre de données où des Éléments de Kyndryl sont présents ou traités, notamment des mesures de détection et de prévention des intrusions et des mesures correctives et d'atténuation des attaques par saturation.

5. Contrôle d'intégrité et de disponibilité des services et des systèmes

5.1 Le Fournisseur s'engage : (a) à réaliser des évaluations des risques liés à la sécurité et la protection des données à caractère personnel, au moins une fois par an, (b) à réaliser des tests de sécurité et à évaluer les vulnérabilités, notamment l'analyse automatisée de la sécurité des systèmes et applications ainsi que le piratage éthique manuel, avant la mise en production et tous les ans par la suite en ce qui concerne les Services et Livrables et tous les ans en lien avec sa Gestion de la Technologie de Kyndryl, (c) à faire appel à un tiers indépendant agréé pour réaliser une fois par an, conformément aux Bonnes pratiques du secteur, des tests d'intrusion comprenant des tests automatisés et manuels, (d) à assurer la gestion automatisée et la vérification de routine de la conformité de chaque composant des Services et Livrables aux exigences de configuration des paramètres de sécurité et en lien avec sa Gestion de la Technologie de Kyndryl et (e) à résoudre les vulnérabilités détectées ou la non-conformité à ses exigences en matière de configuration des paramètres de sécurité en fonction des risques associés, de l'exploitabilité et des impacts. Le Fournisseur prendra des mesures raisonnables pour éviter l'interruption des Services lorsqu'il réalise ses tests, évaluations, analyses et activités de résolution. À la demande de Kyndryl, le Fournisseur transmettra à Kyndryl un rapport récapitulatif écrit sur les activités de test d'intrusion les plus récentes, contenant au minimum le nom des offres couvertes par les tests, le nombre de systèmes ou d'applications admissibles pour les tests, les dates des tests, la méthodologie utilisée dans les tests et un résumé détaillé des résultats.

5.2 Le Fournisseur mettra en place des politiques et procédures destinées à gérer les risques associés à l'application d'éventuelles modifications aux Services ou Livrables ou à la Gestion de la Technologie de Kyndryl. Avant de mettre en œuvre une telle modification, y compris dans les systèmes, réseaux et composants sous-jacents affectés, le Fournisseur consignera dans une demande de modification enregistrée : (a) la description et le motif de la modification, (b) les détails et le planning de l'implémentation, (c) une déclaration de risque traitant de l'impact sur les Services et Livrables, les clients des Services ou les Éléments de Kyndryl, (d) les résultats attendus, (e) le plan d'annulation et (f) l'accord des employés habilités du Fournisseur.

5.3 Le Fournisseur gérera un inventaire de tous les actifs informatiques qu'il utilise lors de l'utilisation des Services, la fourniture des Livrables et la Gestion de la Technologie de Kyndryl. Le Fournisseur surveillera et gérera en continu l'état (y compris la capacité) et la disponibilité desdits actifs informatiques, Services, Livrables et Technologies de Kyndryl, notamment des composants sous-jacents desdits actifs, Services, Livrables et Technologies de Kyndryl.

5.4 Le Fournisseur développera tous les systèmes qu'il utilisera dans le cadre du développement ou de l'utilisation des Services et Livrables et lorsqu'il Gère la Technologie de Kyndryl, à partir de références ou

d'images de sécurité système prédéfinies conformes aux Bonnes pratiques du secteur, par exemple les tests de performances CICS (Center for Internet Security).

5.5 Sans limiter les obligations du Fournisseur ou les droits de Kyndryl au titre du Document de Transaction ou du contrat de base associé entre les parties en lien avec la continuité des opérations, le Fournisseur évaluera séparément chaque Service et Livrable et chaque système informatique utilisé lors de la Gestion de la Technologie de Kyndryl quant aux exigences en matière de continuité des opérations et des systèmes informatiques et aux exigences de reprise après incident conformément aux directives de gestion des risques documentées. Le Fournisseur veillera à ce que chaque Service, Livrable et système informatique comporte, dans les limites garanties par ladite évaluation des risques, des plans de continuité des opérations et des systèmes informatiques et de reprise après incident séparément définis, documentés, gérés et annuellement validés, conformément aux Bonnes pratiques du secteur. Le Fournisseur s'assurera que lesdits plans sont destinés à fournir les temps de reprise énoncés dans l'alinéa 5.6 ci-dessous.

5.6 Les objectifs de point de reprise (« **RPO** ») et les objectifs de temps de reprise (« **RTO** ») en ce qui concerne tout Service Hébergé sont : 24 heures pour les RPO et 24 heures pour les RTO ; cependant, le Fournisseur s'engage à respecter les RPO ou RTO d'une durée inférieure auxquels Kyndryl s'est engagée vis-à-vis d'un Client, immédiatement après la notification écrite envoyée par Kyndryl au Fournisseur l'informant de la durée inférieure des RPO ou des RTO (un e-mail constitue une notification écrite). Pour tous les autres Services que le Fournisseur fournit à Kyndryl, le Fournisseur veillera à ce que des plans relatifs à la continuité des opérations et de reprise après incident soient en place afin d'assurer des RPO et RTO permettant au Fournisseur de respecter toutes ses obligations vis-à-vis de Kyndryl au titre du Document de Transaction et du contrat de base associé entre les parties, et des présentes Conditions, y compris ses obligations d'assurer rapidement le test, le support et la maintenance.

5.7 Le Fournisseur mettra en place des mesures destinées à évaluer, tester et appliquer des correctifs de sécurité recommandés aux Services et Livrables et aux systèmes, réseaux, applications et composants sous-jacents associés dans le périmètre de ces Services et Livrables, ainsi que des systèmes, réseaux, applications et composants sous-jacents utilisés pour Gérer la Technologie de Kyndryl. Une fois que le Fournisseur détermine qu'un correctif de recommandation de sécurité est applicable et approprié, il l'appliquera conformément aux directives d'évaluation des risques et gravités. L'application des correctifs de recommandation de sécurité par le Fournisseur sera soumise à ses politiques en matière de gestion des modifications.

5.8 Si Kyndryl dispose d'arguments lui donnant raisonnablement lieu de considérer que le matériel ou les logiciels fournis à Kyndryl par le Fournisseur peuvent contenir des éléments intrusifs, tels qu'un logiciel espion, un logiciel malveillant ou un code malveillant, le Fournisseur collaborera avec Kyndryl dans les meilleurs délais pour étudier les préoccupations de Kyndryl et les résoudre.

6. Mise à disposition des Services

6.1 Le Fournisseur prendra en charge les méthodes courantes d'authentification fédérée pour les comptes Client ou utilisateur de Kyndryl, en respectant les Bonnes pratiques du secteur lors de l'authentification de ces comptes Client et utilisateur de Kyndryl (par exemple à l'aide de la connexion unique multi-facteur gérée centralement par Kyndryl, en utilisant OpenID Connect ou Security Assertion Markup Language).

7. Sous-traitants. Sans limiter les obligations du Fournisseur ou les droits de Kyndryl au titre du Document de Transaction ou du contrat de base associé entre les parties concernant l'engagement des sous-traitants, le Fournisseur veillera à ce que tout sous-traitant effectuant un travail pour le Fournisseur ait mis en place des contrôles de gouvernance pour se conformer aux exigences et obligations imposées au Fournisseur par les présentes Conditions.

8. Supports physiques. Le Fournisseur assurera en toute sécurité l'expurgation des supports physiques destinés à être réutilisés avant toute réutilisation et détruira les supports physiques non destinés à être réutilisés, conformément aux Bonnes pratiques du secteur relatives à l'expurgation des supports.

Article IX, Certifications et Rapports des Services Hébergés

Le présent Article s'applique si le Fournisseur fournit à Kyndryl un Service Hébergé.

1.1 Le Fournisseur devra obtenir les certifications ou les rapports suivants dans les délais énoncés ci-dessous:

Certifications/Rapports	**Délais**
En ce qui concerne les Services Hébergés du Fournisseur : Certification de conformité ISO 27001, Technologie de l'Information, Techniques de Sécurité, systèmes de gestion de la sécurité de l'information ; cette certification est fondée sur l'évaluation d'un auditeur indépendant réputé. **ou** Norme SOC 2 de Type 2 : un rapport émanant d'un auditeur indépendant réputé faisant état de son évaluation des systèmes, contrôles et opérations du Fournisseur conformément à la norme SOC 2 de Type 2 (y compris au minimum en matière de Sécurité, confidentialité et disponibilité).	Le Fournisseur se procurera une certification ISO 27001 sous 120 jours à partir de la Date d'Entrée en Vigueur du Document de Transaction* ou de sa Date d'Entrée en Vigueur Présumée** et veillera à son renouvellement tous les 12 mois sur la base de l'évaluation d'un auditeur indépendant réputé (conformément à la version la plus récente de la norme). Le Fournisseur se procurera le rapport de conformité SOC 2 de Type 2 sous 240 jours suivant la Date d'Entrée en Vigueur du Document de Transaction* ou de sa Date d'Entrée en Vigueur Présumée**, puis fera réaliser un nouveau rapport par auditeur indépendant réputé, faisant état de son évaluation des systèmes, contrôles et opérations du Fournisseur conformément à la norme SOC 2 de Type 2 (y compris au minimum en matière de Sécurité, confidentialité et disponibilité), tous les 12 mois. * Si, à ladite Date d'Entrée en Vigueur, le Fournisseur fournit un Service Hébergé ** Date à laquelle le Fournisseur présume qu'il assume une obligation de fournir un Service Hébergé

1.2 Sous réserve de la demande écrite du Fournisseur et de l'accord écrit de Kyndryl, le Fournisseur est autorisé à obtenir une certification ou un rapport substantiellement équivalent à ceux indiqués ci-dessus, étant entendu que les délais indiqués dans le tableau ci-dessus s'appliqueront sans modification en ce qui concerne la certification ou le rapport substantiellement équivalent.

1.3 Le Fournisseur sera tenu : (a) à la demande de Kyndryl, de fournir rapidement une copie de chaque certification et rapport qu'il est tenu d'obtenir ; (b) de résoudre dans les meilleurs délais toute vulnérabilité dans les contrôles en interne relevée lors des examens relatifs à la norme SOC 2 ou à toute norme substantiellement équivalente (sous réserve de l'approbation de Kyndryl).

Article X, Coopération, Vérification et Résolution

Le présent Article s'applique si le Fournisseur fournit à Kyndryl des Services ou Livrables.

1. Coopération du Fournisseur

1.1 Si Kyndryl a des raisons de se demander si des Services ou Livrables ont contribué, contribuent ou contribueront à un problème de cybersécurité, le Fournisseur coopérera à toute demande de Kyndryl en lien avec ledit problème, 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.

1.2 Les parties acceptent : (a) de se fournir mutuellement toute autre information demandée par l'une d'elles, (b) de signer et remettre l'une à l'autre tout autre document et (c) de prendre toute autre mesure raisonnable demandée par l'autre partie en vue de l'application des présentes Conditions et des documents mentionnés dans les présentes Conditions. Par exemple, à la demande de Kyndryl, le Fournisseur transmettra, dans les meilleurs délais, les conditions de confidentialité et de sécurité de ses contrats écrits avec ses Sous-traitants ultérieurs et sous-traitants, notamment, si le Fournisseur a le droit de le faire, en donnant accès aux contrats proprement dits.

1.3 Sur demande de Kyndryl, le Fournisseur transmettra, dans les meilleurs délais, des informations sur les pays dans lesquels ses Livrables et les composants de ses Livrables ont été fabriqués, développés ou acquis d'une autre manière.

2. Vérification (le terme « Installation », tel qu'il est utilisé ci-dessous, signifie un emplacement physique dans lequel le Fournisseur héberge ou traite les Éléments de Kyndryl ou y accède)**.**

2.1. Le Fournisseur tiendra à jour un registre pouvant faire l'objet d'un audit et démontrant son respect des présentes Conditions.

2.2 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. 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.

2.3. Une vérification ne peut avoir lieu plus d'une fois par période de douze (12) mois, sauf si (a) la vérification a pour objet la validation d'une rectification par le Fournisseur des problèmes constatés lors d'une précédente vérification pendant la période de douze (12) mois ou si (b) une Violation de Sécurité est survenue et Kyndryl souhaite vérifier la conformité aux obligations relatives à la violation. Dans ces deux cas, Kyndryl adressera le même préavis écrit de trente (30) Jours indiqué dans l'alinéa 2.2 ci-dessus, mais le caractère urgent de la résolution d'une Violation de Sécurité peut nécessiter une vérification par Kyndryl moyennant un préavis écrit inférieur à trente (30) Jours.

2.4. Une autorité compétente ou tout Autre Responsable de traitement peut exercer les mêmes droits octroyés à Kyndryl par les alinéas 2.2 et 2.3, étant entendu qu'une autorité compétente est autorisée à exercer tout autre droit supplémentaire dont elle dispose en vertu de la loi.

2.5. 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.

3. Programme de lutte contre la Contrefaçon

3.1. Si les Livrables du Fournisseur contiennent des composants électroniques (par exemple, disques durs, disques SSD, mémoire, unités centrales, dispositifs logiques ou câbles), le Fournisseur mettra en place et respectera un programme documenté de prévention de la contrefaçon afin, en premier lieu, d'empêcher le Fournisseur de fournir à Kyndryl des composants contrefaits et, en second lieu, de détecter et résoudre rapidement toute situation où le Fournisseur a fourni par erreur à Kyndryl des composants contrefaits. Le Fournisseur imposera cette même obligation de mettre en place et de respecter un programme documenté de prévention de la contrefaçon à tous ses fournisseurs qui fournissent des composants électroniques inclus dans les Livrables du Fournisseur à Kyndryl.

4. Résolution

4.1 En cas de manquement du Fournisseur à l'une quelconque de ses obligations stipulées dans les présentes Conditions et si ce manquement occasionne une Violation de Sécurité, le Fournisseur devra remédier à ce manquement et résoudre les effets préjudiciables de la Violation de Sécurité selon les instructions et les délais raisonnables de Kyndryl. Toutefois, si la Violation de Sécurité découle de la mise à disposition par le Fournisseur d'un Service Hébergé partagé, et affecte par conséquent de nombreux clients du Fournisseur, y compris Kyndryl, le Fournisseur, compte tenu de la nature de la Violation de Sécurité, corrigera rapidement et de manière appropriée cette défaillance dans son exécution et remédiera aux effets préjudiciables de la Violation de Sécurité, tout en tenant dûment compte de toute remarque de Kyndryl sur ces corrections et cette résolution. Sans préjudice de ce qui précède, le Fournisseur doit avertir Kyndryl sans délai indu si le Fournisseur n'est plus en mesure de respecter les obligations fixées par la législation applicable en matière de protection des données.

4.2 Kyndryl aura le droit de participer à la résolution de toute Violation de Sécurité référencée à la Section 4.1, de la manière qu'elle estimera appropriée ou nécessaire, et le Fournisseur sera responsable des coûts et dépenses relatifs à la correction dans son exécution, et des coûts et dépenses de résolution des parties en lien avec la Violation de Sécurité.

4.3 À titre d'exemple, les coûts et dépenses de résolution associés à une Violation de Sécurité peuvent inclure ceux permettant de détecter et d'étudier une Violation de Sécurité, de déterminer les responsabilités au titre des lois et réglementations applicables, de fournir des notifications de violation, d'établir et de gérer des centres d'appels, de fournir des services de suivi de crédit et de rétablissement de crédit, de recharger les données, de corriger les défauts de produit (y compris par le biais du développement de code source ou autre), de faire appel à des tiers pour faciliter les activités susmentionnées ou autres activités pertinentes, ainsi que les autres coûts et dépenses nécessaires pour remédier aux effets préjudiciables de la Violation de Sécurité. Par souci de clarté, les coûts et dépenses de résolution n'incluent pas les pertes de bénéfices, d'activité commerciale, de valeur, de revenu, de clientèle ou d'économies escomptées par Kyndryl.