Principes de Sécurité et de Protection des Données Kyndryl

1. Définitions

Les termes en majuscules employés dans le présent document sont définis ci-dessous. Si tel n'est pas le cas, les définitions sont indiquées dans le contrat applicable entre Kyndryl et le Client pour les Services Kyndryl.

Le Client – désigne l'entité à laquelle Kyndryl fournit les Services Kyndryl dans le cadre d'un Document de Services Kyndryl.

Les Composants – sont les éléments d'application, de plateforme ou d'infrastructure d'un Service Kyndryl mis en oeuvre et géré par Kyndryl.

Le Contenu – désigne l'ensemble des données, logiciels et informations auxquels le Client ou ses utilisateurs agréés autorisent l'accès, ou qu'ils fournissent ou transmettent aux Services Kyndryl.

Le DSP – désigne le présent document sur les Principes de Sécurité et de Protection des Données Kyndryl.

Le Document de Services Kyndryl – est un Document de Transaction et tout autre document intégré dans un contrat entre Kyndryl et un Client, et qui fournit des détails sur un Service Kyndryl en particulier.

Les Services Kyndryl – sont (a) les offres de services Kyndryl, y compris les offres de service d'infrastructure ou d'application que Kyndryl fournit ou personnalise pour un Client et (b) tout autre service, y compris les conseils, la maintenance ou l'assistance que Kyndryl fournit à un Client.

L'Incident de Sécurité est un accès non autorisé et une utilisation non autorisée du Contenu.

Le Document de Transaction – est un document qui donne des détails sur les transactions, comme le prix et une description, ainsi que des informations sur un Service Kyndryl. Parmi les exemples de Documents de Transaction, figurent les descriptifs et les descriptions de service, les bons de commande et les factures pour un Service Kyndryl. Plusieurs Documents de Transaction peuvent être applicables à une transaction.

2. Présentation

Les mesures techniques et organisationnelles indiquées dans le présent DSP s'appliquent aux Services Kyndryl (y compris aux Composants) uniquement dans les cas où Kyndryl a expressément donné son accord pour se conformer au DSP dans un contrat entre Kyndryl et le Client. Pour plus de clarté, ces mesures ne s'appliquent pas dans les cas où le Client est responsable de la sécurité et de la confidentialité, ou tel que spécifié ci-dessous ou dans un Document de Service Kyndryl.

a. Il incombe au Client de déterminer si un Service Kyndryl est adapté à l'utilisation qui en est faite par lui et de mettre en place et gérer des mesures de sécurité et de confidentialité pour des composants non fournis et non gérés par Kyndryl dans le cadre des Services Kyndryl. Les responsabilités du Client par rapport aux Services Kyndryl incluent notamment : (1) la sécurité des systèmes et des applications conçus ou déployés par le Client dans le cadre d'une offre d'infrastructure en tant que service ou plateforme en tant que service, ou dans le cadre d'une infrastructure, de Composants ou de logiciels que Kyndryl gère pour un Client, et (2) la configuration de la sécurité au niveau de l'application et le contrôle de l'accès de l'utilisateur final du Client pour une offre de logiciel en tant que service que Kyndryl gère pour un Client ou une offre de service d'application que Kyndryl fournit à un Client.

b. Le Client reconnaît que Kyndryl peut, de temps à autre et à son entière discrétion, modifier le présent DSP et que de telles modifications remplaceront les versions précédentes à compter de la date de publication par Kyndryl de la version modifiée. Nonobstant toute mention contraire dans tout contrat écrit entre Kyndryl et le Client, les modifications auront pour objectif : (1) d'améliorer ou de clarifier les engagements existants, (2) de permettre à Kyndryl de hiérarchiser de façon appropriée la sécurité afin de gérer les menaces et les problèmes changeants relatifs à la cybersécurité et aux données, (3) de maintenir la conformité aux normes actuelles et aux lois applicables ou (4) de fournir des dispositifs et des fonctionnalités supplémentaires. Les modifications ne dégraderont pas les dispositifs ou fonctionnalités de sécurité ou de protection de données des Service Kyndryl.

c. En cas de conflit entre le présent DSP et un Document de Services Kyndryl, le Document de Services Kyndryl prévaut et si les termes à l'origine du conflit se trouvent dans un Document de Transaction, ils prévaudront sur les termes du présent DSP et s'appliqueront uniquement à la transaction spécifique.

3. Protection des Données

a. Kyndryl traitera l'ensemble du Contenu comme confidentiel en ne divulguant le Contenu qu'aux employés, sous-traitants et fournisseurs (y compris les sous-traitants ultérieurs) de Kyndryl, et uniquement dans la mesure où cela est nécessaire pour fournir les Services Kyndryl.

b. Les mesures de sécurité et de confidentialité appliquées à chaque Service Kyndryl sont mises en oeuvre conformément aux principes relatifs à la sécurité et la protection des données dès la conception de Kyndryl (« Security and Privacy by design ») afin de protéger le Contenu traité par un Service Kyndryl et de maintenir la disponibilité dudit Contenu conformément au contrat applicable entre Kyndryl et le Client, y compris les Documents de Services Kyndryl.

c. Des informations supplémentaires sur la sécurité et la confidentialité propres à un Service Kyndryl peuvent être disponibles dans le Document de Services Kyndryl associé ou dans d'autres documents standard pour aider à l'évaluation initiale et continue de l'adéquation d'un Service Kyndryl à son utilisation par le Client. Ces informations peuvent comprendre des preuves d'accréditations et de certifications déclarées, des informations relatives auxdites accréditations et certifications, des feuilles de données, des FAQ et d'autres documentations généralement disponibles. Kyndryl dirigera le Client vers la documentation standard disponible s'il est nécessaire de remplir des questionnaires relatifs à la sécurité ou à la confidentialité selon le choix du Client.

4. Politiques de Sécurité

a. Kyndryl maintiendra et respectera les politiques et pratiques écrites en matière de sécurité informatique qui font partie intégrante des activités de Kyndryl et sont obligatoires pour tous les employés de Kyndryl. Le Responsable de la Sécurité des Systèmes d'Information de Kyndryl (Kyndryl Chief Information Security Officer) assumera la responsabilité et la supervision de l'exécution de ces politiques, notamment la gouvernance formelle et la gestion des révisions, la formation des employés et l'application de la conformité.

b. Kyndryl passera en revue ses politiques de sécurité informatique au moins une fois par an et les modifiera selon ce que Kyndryl juge raisonnable pour maintenir la protection des Services et du Contenu Kyndryl.

c. Kyndryl maintiendra et respectera ses obligations d'attestation d'emploi standard pour tous les nouveaux employés et étendra lesdites obligations à ses filiales détenues à 100 %. Conformément aux processus et procédures internes de Kyndryl, ces exigences seront examinées périodiquement et comprennent notamment des vérifications de casier judiciaire, la validation de l'identité ainsi que d'autres contrôles jugés nécessaires par Kyndryl. Chaque société Kyndryl est responsable de la mise en œuvre de ces exigences dans le cadre de ses procédures de recrutement si elles sont applicables et dans la limite de la législation locale.

d. Les employés de Kyndryl effectueront chaque année une formation dans les domaines de la sécurité et la protection des Données à caractère personnel et certifieront chaque année qu'ils respecteront les politiques de Kyndryl en matière d'éthique professionnelle, de confidentialité et de sécurité, telles qu'elles sont exposées dans le document Kyndryl intitulé « Principes de conduite dans les affaires ». Une formation supplémentaire sera dispensée aux personnes ayant un accès administrateur aux Composants spécifiques à leur rôle dans le cadre de l'exploitation et de la prise en charge du Service par Kyndryl et comme requis pour maintenir la conformité et les accréditations énoncées dans tout Document de Services Kyndryl.

5. Conformité

a. Kyndryl maintiendra la conformité et l'accréditation pour les Services Kyndryl tel que défini dans un Document de Service Kyndryl.

b. Sur demande, Kyndryl apportera une preuve de la conformité et de l'accréditation énoncées au point 5a, par exemple des certificats, attestations ou rapports résultant des audits de tiers agréés indépendants (des audits indépendants de tiers accrédités auront lieu à la fréquence requise par la norme applicable).

c. Kyndryl est responsable de ces mesures de sécurité et de confidentialité des données même si Kyndryl fait appel à un sous-traitant ou un fournisseur (y compris les sous-traitants ultérieurs) pour la livraison ou la prise en charge d'un Service Kyndryl.

6. Incidents de Sécurité

a. Kyndryl maintiendra et respectera les politiques de résolution d'incident documentées, conformément aux directives du National Institute of Standards and Technology du Département du Commerce des États-Unis (NIST) ou des normes équivalentes relatives au traitement des incidents de sécurité informatique et respectera les dispositions du contrat applicable entre Kyndryl et le Client relatives à la notification de violation de données.

b. Kyndryl enquêtera sur les Incidents de Sécurité dont Kyndryl viendrait à avoir connaissance et, dans le cadre des Services Kyndryl, Kyndryl définira et exécutera un plan d'intervention approprié. Le Client peut notifier à Kyndryl une vulnérabilité ou un incident présumé en soumettant une demande dans le cadre du processus de rapport d'incidents spécifique aux Services Kyndryl (tel qu'indiqué dans un Document de Services Kyndryl) ou, en l'absence d'un tel processus, en soumettant une demande de support technique.

c. Kyndryl notifiera au Client, sans retard injustifié, un Incident de Sécurité connu ou raisonnablement présumé par Kyndryl comme ayant un impact sur le Client. Kyndryl fournira au Client des informations que celui-ci est raisonnablement en droit de demander sur ledit Incident de Sécurité et sur l'état de toutes activités de résolution et de restauration de Kyndryl.

7. Sécurité Physique et Contrôle d'Entrée

a. Kyndryl maintiendra des 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 gérées par Kyndryl (centres de données) utilisées pour héberger les Services Kyndryl. Les points d'entrée auxiliaires dans ces centres de données, tels que les zones de livraison et les plateformes de chargement, seront contrôlés et isolés des ressources informatiques.

b. L'accès aux centres de données gérés par Kyndryl et aux zones contrôlées au sein de ces centres de données sera limité par fonction et soumis à l'accord de personnes habilitées. Ces accès seront consignés dans des journaux qui seront conservés pendant au moins un an. Kyndryl révoquera l'accès aux zones contrôlées d'un centre de données géré par Kyndryl dès la rupture du contrat de travail d'un employé habilité. Kyndryl 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.

c. Toute personne ayant dûment reçu l'autorisation temporaire d'accéder aux locaux d'un centre de données géré par Kyndryl ou à une zone contrôlée au sein d'un centre de données sera enregistrée dès son arrivée dans les locaux, doit présenter une preuve d'identité lors de son enregistrement et sera accompagnée par le personnel autorisé. Toute autorisation temporaire d'entrée, y compris les livraisons, sera planifiée d'avance et doit être approuvée par le personnel autorisé.

d. Kyndryl prendra les précautions nécessaires pour protéger l'infrastructure physique des locaux du centre de données géré par Kyndryl contre les menaces environnementales, tant d'origine naturelle qu'humaine, par exemple température ambiante excessive, incendie, inondation, humidité, vol et vandalisme.

8. Contrôle d'Accès, d'Intervention, de Transfert et de Séparation

a. Kyndryl passera en revue ladite architecture de sécurité, y compris les mesures destinées à empêcher les connexions réseau non autorisées aux systèmes, applications et périphériques réseau, afin de garantir la conformité à ses normes en matière de segmentation sécurisée, d'isolement et de protection complète avant l'implémentation.

b. Kyndryl peut utiliser la technologie de réseau sans fil dans le cadre de la maintenance et la prise en charge des Services Kyndryl et des Composants associés. Ces réseaux sans fil, le cas échéant, seront chiffrés et nécessiteront une authentification sécurisée.

c. Kyndryl maintiendra, pour un Service Kyndryl, des mesures destinées à séparer logiquement le Contenu et à empêcher que ce dernier soit exposé ou accessible aux personnes non autorisées. Kyndryl maintiendra une isolation appropriée de ses environnements de production et hors production et, si le Contenu est transféré vers un environnement hors production, par exemple pour reproduire une erreur à la demande du Client, la protection en termes de sécurité et de confidentialité dans l'environnement hors production sera équivalente à celle de l'environnement de production.

d. Kyndryl chiffrera le Contenu non destiné au grand public ou à une consultation non authentifiée lorsqu'elle transfère le Contenu sur les réseaux publics et permettra l'utilisation d'un protocole cryptographique, tel que HTTPS, SFTP et FTPS, pour le transfert sécurisé du Contenu par le Client à destination et en provenance des Services Kyndryl sur les réseaux publics.

e. Kyndryl chiffrera le Contenu stocké dans la mesure où cela est spécifié dans un Document de Services Kyndryl. Si le Service Kyndryl inclut la gestion de clés cryptographiques, Kyndryl maintiendra 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 des clés sécurisées.

f. Si Kyndryl requiert l'accès au Contenu pour fournir les Services Kyndryl, et si un tel accès est géré par Kyndryl, Kyndryl restreindra et limitera cet accès au niveau minimum requis. Ledit accès, y compris l'accès administrateur aux Composants sous-jacents (accès privilégié) sera individuel, défini en fonction des rôles et soumis à l'accord et la validation régulière du personnel Kyndryl autorisé conformément aux principes de séparation des tâches. Kyndryl maintiendra des mesures permettant d'identifier et de supprimer les comptes redondants et inactifs dotés de l'accès privilégié et révoquera ledit accès dans les plus brefs délais dès la rupture du contrat de travail du propriétaire de compte ou à la demande du personnel Kyndryl autorisé, par exemple le manager du propriétaire de compte.

g. Conformément aux normes standard du secteur d'activité et dans les limites nativement prises en charge par chaque Composant, Kyndryl maintiendra 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 une phrase passe fiable, ainsi que des mesures nécessitant le transfert et le stockage sécurisés desdits mots de passe et phrases passe.

h. Kyndryl surveillera l'utilisation des accès privilégiés et tiendra à jour les informations de sécurité et les mesures de gestion d'événement destinées à : (1) identifier les accès et activités non autorisés, (2) faciliter une réponse rapide et appropriée et (3) permettre des audits de tiers internes et indépendants de la conformité aux politiques documentées de Kyndryl.

i. Les journaux dans lesquels les activités et accès privilégiés sont consignés seront conservés conformément à la politique de Kyndryl. Kyndryl maintiendra des mesures de protection contre l'accès non autorisé, la modification et la destruction accidentelle ou délibérée desdits journaux.

j. Dans les limites prises en charge par les fonctionnalités natives des périphériques et du système d'exploitation, Kyndryl gérera des dispositifs de protection informatique pour ses systèmes d'utilisateur final comprenant notamment des pare-feux d'extrémité, le chiffrement de disque complet, la détection et la suppression de logiciels malveillants, les verrouillages d'écran temporels et les solutions de gestion de nœud final imposant des obligations d'application de correctif et de configuration des paramètres de sécurité.

k. Kyndryl 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 directives NIST relatives à l'expurgation des supports.

9. Contrôle d'Intégrité et de Disponibilité des Services

a. Kyndryl s'engage à : (1) réaliser des évaluations des risques liés à la sécurité et la confidentialité des Services Kyndryl au moins une fois par an ; (2) réaliser des tests de sécurité et évaluer les vulnérabilités des Services Kyndryl avant la mise en production, puis au moins une fois par an par la suite, (3) réaliser les tests d'intrusion des fonctionnalités et des offres avant la mise en production, puis une fois par an, (4) assurer la détection automatisée des vulnérabilités des Composants sous-jacents des Services Kyndryl conformément aux meilleures pratiques en termes de configuration de la sécurité du secteur, (5) résoudre les vulnérabilités détectées par les analyses ou les tests de sécurité en fonction du risque, de l'exploitabilité et de l'impact associés et (6) prendre des mesures raisonnables afin d'éviter les perturbation des Services Kyndryl lors de la réalisation des tests, évaluations, analyses et mise en place des activités de remédiations.

b. Kyndryl maintiendra des mesures destinées à évaluer, tester et appliquer des correctifs de recommandations de sécurité aux Services Kyndryl et aux systèmes, réseaux, applications et Composants sous-jacents associés dans le périmètre des Services Kyndryl. Une fois que Kyndryl détermine qu'un correctif de recommandations de sécurité est applicable et approprié, Kyndryl l'appliquera conformément aux directives d'évaluation des risques et gravités en fonction du Système d'évaluation des correctifs Common Vulnerability Scoring, lorsque disponible. La mise en oeuvre des

correctifs de recommandation de sécurité sera soumise aux politiques de Kyndryl en matière de gestion des modifications.

c. Kyndryl maintiendra des politiques et procédures destinées à gérer les risques associés à l'application de modifications aux Services Kyndryl. Avant l'implémentation, les modifications apportées à un Service Kyndryl, y compris ses systèmes, réseaux et Composants sous-jacents, seront consignées dans une demande de modification enregistrée comprenant la description et le motif de la modification, les détails et le planning de l'implémentation, une déclaration de risque abordant l'impact sur le Service Kyndryl et ses clients, les résultats attendus, le plan d'annulation et l'accord documenté du personnel autorisé.

d. Kyndryl gérera un inventaire de tous les actifs informatiques utilisés pour la mise en oeuvre des Services Kyndryl. Kyndryl surveillera et gèrera en continu l'état, y compris la capacité et la disponibilité des Services Kyndryl et des Composants sous-jacents.

e. Chaque Service Kyndryl sera évalué séparément quant aux exigences en matière de continuité des opérations et de reprise après incident par le biais d'une analyse d'impact sur les activités et des évaluations des risques appropriées en vue d'identifier et de hiérarchiser les fonctions essentielles aux activités. Chaque Service Kyndryl comportera, dans les limites garanties par ladite évaluation des risques, des plans de continuité des opérations et de reprise après incident séparément définis, documentés, gérés et annuellement validés, conformément aux pratiques en vigueur dans le secteur d'activité. Les objectifs de point de reprise et de temps de reprise du Service Kyndryl, s'ils sont fournis dans le Document de Services Kyndryl, seront établis en tenant compte de l'architecture et de l'usage prévu du Service Kyndryl. Les supports physiques destinés au stockage hors site, le cas échéant, comme les supports contenant des fichiers de sauvegarde, seront chiffrés avant le transport.