Стаття I. Інформація про ділові контакти

Ця Стаття застосовується, якщо Постачальник або Kyndryl обробляє BCI іншої сторони.

1.1 Kyndryl і Постачальник можуть обробляти BCI іншої сторони при веденні бізнесу у зв'язку з наданням Постачальником Послуг і Результатів.

1.2 Сторона:

(a) зобов'язується не використовувати та не розкривати BCI іншої сторони з будь-якою іншою метою (для ясності: жодна зі сторін не повинна Продавати BCI іншої сторони, використовувати або розкривати BCI іншої сторони для будь-яких маркетингових цілей без попередньої письмової згоди іншої сторони і в необхідних випадках — без попередньої письмової згоди відповідних Суб'єктів Даних), і

(b) зобов'язується видаляти, змінювати, виправляти, повертати, надавати інформацію про Обробку, обмежувати Обробку або вживати будь-яких інших обґрунтовано затребуваних дій щодо BCI іншої сторони негайно за письмовим запитом іншої сторони, коли будь-яке несанкціоноване використання особистої інформація виникає, і сторона хоче припинити обробку та виправити.

1.3 Сторони не встановлюють між собою відносини спільного Володільця BCI одна одної, і жодне положення Документа Транзакції не буде тлумачитися або розцінюватися як таке, що свідчить про будь-який намір встановити відносини спільного Володільця.

1.4 Додаткові відомості про Обробку Kyndryl BCI наведено в Заяві Kyndryl про конфіденційність, опублікованій на сайті https://www.kyndryl.com/us/en/privacy.

1.5 Сторони запровадили і зобов'язуються підтримувати технічні та організаційні заходи безпеки для захисту BCI від втрати, знищення, зміни, випадкового або несанкціонованого розкриття, випадкового або несанкціонованого доступу та незаконної Обробки.

1.6 Постачальник зобов'язується невідкладно (але в жодному разі не пізніше ніж протягом 48 годин) повідомити Kyndryl, щойно йому стане відомо про будь-яке Порушення Безпеки, що стосується BCI Kyndryl. Постачальник надаватиме таке повідомлення за адресоюcyber.incidents@kyndryl.com. Постачальник зобов'язаний надати на обґрунтований запит Kyndryl інформацію щодо такого порушення та будь-яких дій Постачальника, спрямованих на виправлення та відновлення діяльності. Наприклад, обґрунтовано запитувана інформація може включати журнали, що підтверджують доступ привілейованих користувачів, адміністраторів та інших користувачів до Пристроїв, систем або прикладних програм, образів для експертного аналізу Пристроїв, систем або прикладних програм та інші подібні елементи, наскільки вони стосуються порушення або його виправлення Постачальником і відновлення діяльності.

1.7 Якщо Постачальник Обробляє лише BCI Kyndryl і не має доступу до будь-яких інших даних або матеріалів будь-якого типу або до будь-якої Корпоративної Системи Kyndryl, то до такої Обробки застосовуються тільки ця Стаття та Стаття X (Співпраця, перевірка та виправлення).

Стаття II. Технічні та організаційні заходи, Захист даних

Ця Стаття застосовується, якщо Постачальник здійснює Обробку Даних Kyndryl, інших ніж ВСІ Kyndryl. Постачальник зобов'язаний виконувати вимоги цієї Статті під час надання всіх Послуг і Результатів і таким чином захищати Дані Kyndryl від втрати, знищення, зміни, випадкового або несанкціонованого розкриття, випадкового або несанкціонованого доступу та незаконних форм Обробки. Вимоги цієї Статті поширюються на всі прикладні програми, платформи та інфраструктуру ІТ, функціонування яких і управління якими забезпечує Постачальник під час надання Результатів і Послуг, включаючи всі послуги розробки, тестування, розміщення, підтримки, експлуатації та середовища центрів обробки даних.

1. Використання Даних

1.1 Постачальник не може додавати до Даних Kyndryl або включати разом із Даними Kyndryl будь-яку іншу інформацію або дані, зокрема будь-які Персональні Дані, без попередньої письмової згоди Kyndryl? і Постачальник не може використовувати Дані Kyndryl у будь-якій формі, зокрема у зведеній або іншій формі, для будь-яких інших цілей, окрім надання Послуг і Результатів (наприклад, Постачальнику забороняється використовувати або повторно використовувати Дані Kyndryl для оцінки ефективності або заходів удосконалення пропозицій Постачальника, для дослідження та розробки з метою створення нових пропозицій або для створення звітів стосовно пропозицій Постачальника). Якщо це прямо не дозволено в Документі Транзакції, Постачальнику заборонено Продавати Дані Kyndryl.

1.2 Постачальник зобов'язується не включати будь-які технології для відстеження в Інтернеті в Результати або Послуги (такі технології включають HTML5, локальне сховище, теги або маркери третіх осіб і веб-маяки), якщо це прямо не дозволено в Документі Транзакції.

2. Запити Третіх Осіб і Конфіденційність

2.1 Постачальник розкриватиме Дані Kyndryl третім особам тільки за умови отримання попереднього письмового дозволу Kyndryl. Якщо органи державної влади, включаючи будь-які регуляторні органи, вимагають надання їм доступу до Даних Kyndryl (наприклад, якщо уряд США видає Постачальнику ордер Служби національної безпеки США на отримання Даних Kyndryl) або якщо розкриття Даних Kyndryl є обов'язковим відповідно до вимог законодавства, Постачальник зобов'язується письмово повідомити Kyndryl про таку вимогу та надати Kyndryl достатню можливість оскаржити будь-яке розкриття (якщо законодавство забороняє надавати повідомлення, Постачальник зобов'язується вжити заходів, які, на його думку, є доцільними, щоб оскаржити заборону та розкриття Даних Kyndryl у суді або із застосуванням інших засобів).

2.2 Постачальник запевняє Kyndryl, що: (a) лише ті його працівники, які мають службову необхідність у доступі до Даних Kyndryl для надання Послуг або Результатів, матимуть такий доступ, і лише в обсязі, необхідному для надання таких Послуг і Результатів; і (b) він зобов'язав своїх працівників дотримуватися зобов'язань конфіденційності, відповідно до яких такі працівники зобов'язані використовувати та розкривати Дані Kyndryl виключно в порядку, встановленому в цих Положеннях.

3. **Повернення або видалення Даних Kyndryl**

3.1 Постачальник зобов'язаний, за вибором Kyndryl, видалити або повернути Kyndryl Дані Kyndryl після дострокового припинення або закінчення строку дії Документа Транзакції або раніше на вимогу Kyndryl. Якщо Kyndryl вимагає видалити дані, то Постачальник, діючи згідно з Кращими практиками індустрії, повинен зробити дані нечитабельними, щоб їх не можна було знов зібрати або відновити, і підтвердити для Kyndryl факт видалення. Якщо Kyndryl вимагає повернути Дані Kyndryl,

Постачальник повинен повернути їх у встановлений Kyndryl достатній термін та згідно з обґрунтованими письмовими інструкціями Kyndryl.

Стаття III. Конфіденційність

Ця Стаття застосовується, якщо Постачальник здійснює Обробку Персональних Даних Kyndryl.

1. Обробка

1.1 Kyndryl призначає Постачальника Розпорядником Обробки Персональних Даних Kyndryl з єдиною метою надання Результатів і Послуг відповідно до інструкцій Kyndryl, включаючи інструкції, що містяться в цих Положеннях, Документі Транзакції та пов'язаному з ним базовому договорі між сторонами. Якщо Постачальник не виконує інструкції, Kyndryl може припинити споживання відповідної частини Послуг, надавши письмове повідомлення. Якщо Постачальник вважає, що інструкція порушує закони про захист даних, Постачальник зобов'язаний невідкладно повідомити про це Kyndryl у встановлені законодавством строки. Якщо Постачальник не виконує якихось своїх зобов’язань за цими Положеннями і таке невиконання призводить до несанкціонованого використання Персональних Даних або, загалом, до будь-якого несанкціонованого використання Персональних Даних, Kyndryl матиме право припинити обробку, усунути невиконання та виправити негативні наслідки несанкціонованого використання, виконавши відповідні дії та виправлення згідно з обґрунтованими інструкціями та графіком Kyndryl.

1.2 Постачальник дотримуватиметься усіх законів про захист даних, що стосуються Послуг і Результатів.

1.3 Додаток до Документа Транзакції або власне Документ Транзакції встановлює щодо Даних Kyndryl:

(a) категорії Суб'єктів Даних;
(b) типи Персональних Даних Kyndryl;
(c) дії з даними та Дії з обробки;
(d) тривалість і періодичність Обробки; і
(e) список Суброзпорядників.

2. Технічні та Організаційні Заходи

2.1 Постачальник впроваджуватиме та підтримуватиме технічні й організаційні заходи, описані в Статті II (Технічні та організаційні заходи, Захист даних) і Статті VIII (Технічні та організаційні заходи, Загальні параметри безпеки), і забезпечуватиме рівень безпеки, який відповідає ризику, пов'язаному з Послугами та Результатами. Постачальник підтверджує та розуміє обмеження Статті II, цієї Статті III та Статті VIII і зобов'язується їх дотримуватись.

3. Права та Запити Суб'єктів даних

3.1 Постачальник невідкладно (в строки, що дозволяють Kyndryl і будь-яким Іншим Володільцям виконувати їхні зобов'язання, встановлені законодавством), повідомлятиме Kyndryl про всі запити від Суб'єктів Даних, які здійснюють свої права як Суб'єкти Даних (зокрема право на уточнення, видалення або блокування даних), стосовно Персональних Даних Kyndryl. Постачальник також може у найкоротші строки дати вказівку Суб’єкту Даних надіслати такий запит до Kyndryl. Постачальник не відповідатиме на будь-які запити від Суб'єктів Даних, окрім випадків, передбачених законом або письмовими інструкціями від Kyndryl.

3.2 Якщо Kyndryl буде зобов'язана надати інформацію щодо Персональних Даних Kyndryl Іншим Володільцям або третім особам (наприклад, Суб'єктам Даних або регуляторним органам), Постачальник має сприяти Kyndryl у цьому, надавши необхідну інформацію та виконавши інші обґрунтовані дії на запит Kyndryl, у строки, що дозволять Kyndryl своєчасно дати відповідь таким Іншим Володільцям або третім особам.

4. Суброзпорядники

4.1 Постачальник надасть Kyndryl попереднє письмове повідомлення перед додаванням нового Суброзпорядника або розширенням обсягу Обробки існуючим Суброзпорядником, і зазначить у цьому повідомленні назву Суброзпорядника та опис нового або розширеного обсягу Обробки. Kyndryl може у будь-який час заперечити проти будь-якого такого нового Суброзпорядника або розширеного обсягу з обґрунтованих підстав, і якщо Kyndryl скористається таким правом, сторони сумлінно співпрацюватимуть для вирішення заперечень Kyndryl. Із застереженням про право Kyndryl подати таке заперечення в будь-який час, Постачальник може призначити нового Суброзпорядника або розширити обсяг Обробки існуючого Суброзпорядника, якщо Kyndryl не заявила заперечення протягом 30 Днів від дати письмового повідомлення від Постачальника.

4.2 Постачальник встановить зобов'язання щодо захисту даних, безпеки та сертифікації, передбачені в цих Положеннях, для кожного затвердженого Суброзпорядника перед Обробкою Суброзпорядником будь-яких Даних Kyndryl. Постачальник несе повну відповідальність перед Kyndryl за виконання зобов'язань кожним Суброзпорядником.

5. Транскордонна Обробка Даних

Нижченаведені терміни вживаються в такому значенні:

Країна з належним рівнем захисту: країна, яка забезпечує належний рівень захисту даних під час передачі відповідно до застосовного законодавства про захист даних або рішень регуляторних органів.

Імпортер Даних: Розпорядник або Суброзпорядник, зареєстрований не в Країні з належним рівнем захисту.

Стандартні договірні положення ЄС («СДП ЄС»): Стандартні договірні положення ЄС (Рішення комісії 2021/914) із застосуванням необов'язкових позицій, за винятком опції 1 Пункту 9(a) та опції 2 Пункту 17, які офіційно опубліковані за адресою https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Стандартні договірні положення Сербії («СДП Сербії»): Стандартні договірні положення Сербії, прийняті «Уповноваженим Сербії щодо інформації, що становить публічний інтерес, та захисту персональних даних», які опубліковані на сайті https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Стандартні договірні умови («**СДП**»): договірні умови, що вимагаються відповідним законодавством щодо передачі Персональних Даних Розпорядникам, зареєстрованим не в Країнах із належним рівнем захисту.

Доповнення Сполученого Королівства про міжнародну передачу даних до Стандартних договірних положень ЄС («Доповнення СК»): Доповнення Сполученого Королівства про міжнародну передачу даних до Стандартних договірних положень ЄС, офіційно опубліковане на сайті https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

Доповнення Швейцарії до Стандартних договірних положень ЄС («Доповнення Швейцарії»): договірні положення до Стандартних договірних положень ЄС, які застосовуються відповідно до рішення Швейцарського агентства з захисту даних (**Федерального уповноваженого з захисту даних та інформації — «FDPIC»**) і відповідно до Федерального закону Швейцарії про захист даних (**«FADP»**).

5.1 Постачальник зобов'язаний не передавати і не розкривати (включаючи шляхом віддаленого доступу) будь-які Персональні Дані Kyndryl за межі країни без попередньої письмової згоди Kyndryl. Якщо Kyndryl надасть таку згоду, сторони співпрацюватимуть для забезпечення дотримання чинного законодавства про захист даних. Якщо таким законодавством передбачено укладення SCC, Постачальник невідкладно укладе SCC на вимогу Kyndryl.

5.2 Стосовно СДП ЄС:

(a) Якщо Постачальник зареєстрований не в Країні з належним рівнем захисту: Постачальник укладає СДП ЄС із Kyndryl як Імпортер Даних, і Постачальник повинен укласти письмові договори з кожним затвердженим Суброзпорядником відповідно до Пункту 9 СДП ЄС, а також надати компанії Kyndryl копії таких договорів на її запит.

(i) Модуль 1 СДП ЄС не застосовується, якщо інше не узгоджено в письмовому вигляді.

(ii) Модуль 2 СДП ЄС застосовується, якщо Kyndryl є Володільцем, а Модуль 3 — якщо Kyndryl є Розпорядником. Відповідно до Пункту 13 СДП ЄС, коли застосовуються Модулі 2 або 3, сторони погоджуються з тим, що (1) СДП ЄСрегулюються законодавством країни-учасниці ЄС, де знаходиться компетентний уповноважений наглядовий орган, і (2) будь-які суперечки, які виникають на основі СДП ЄС, вирішуватимуться в судах країни-учасниці ЄС, де знаходиться компетентний уповноважений наглядовий орган. Якщо таке законодавство в (1) не допускає права третіх осіб-бенефіціарів, тоді СДП ЄС регулюються законодавством Нідерландів, і будь-які суперечки, що виникають на основі СДП ЄС, (2) вирішуються в суді Амстердама (Нідерланди).

(b) Якщо обидві сторони, Постачальник і Kyndryl, зареєстровані в Країні з належним рівнем захисту, Постачальник діятиме в якості Експортера даних і укладатиме СДП ЄС з кожним затвердженим Суброзпорядником у Країні з неналежним рівнем захисту. Постачальник виконуватиме необхідну Оцінку впливу передачі даних (Transfer Impact Assessment, TIA) і без зайвого зволікання повідомить Kyndryl про (1) будь-яку необхідність застосування додаткових заходів і (2) про застосовані заходи. За запитом Постачальник надасть компанії Kyndryl результати TIA та усю інформацію, необхідну для розуміння та оцінки результатів. У разі непогодження Kyndryl з результатами TIA Постачальника або застосованими додатковими заходами Kyndryl і Постачальник співпрацюватимуть над пошуком прийнятного рішення. Kyndryl зберігає за собою право призупинити або припинити відповідні Послуги Постачальника без оплати. Щоб уникнути непорозумінь, уточнюємо: це не звільняє Суброзпорядників Постачальника від зобов’язання стати стороною СДП ЄС з Kyndryl або Замовниками, як зазначено в розділі 5.2 (d) нижче.

(c) Якщо Постачальник зареєстрований у країні, що є учасником Європейського Економічного Простору, а Kyndryl виступає в якості Володільця, на якого не розповсюджуються вимоги Загального Регламенту про Захист Даних 2016/679, тоді застосовується Модуль 4 СДП ЄС, і Постачальник цим укладає СДП ЄС із Kyndryl як експортер даних. Якщо застосовується Модуль 4 СДП ЄС, тоді сторони погоджуються, що СДП ЄС регулюватимуться законодавством Нідерландів, і будь-які суперечки, що виникають на основі СДП ЄС, вирішуватимуться в суду Амстердама (Нідерланді).

(d) Якщо Інші Володільці, наприклад Замовники або афілійовані особи, надсилають запит стати стороною СДП ЄС відповідно до особливої умови Пункту 7, Постачальник цим погоджується з будь-яким таким запитом.

(e) Технічні та Організаційні Заходи, які є обов’язковими для заповнення Доповнення II до СДП ЄС, можна знайти в цих Положеннях, самому Транзакційному Документі, а також у відповідному базовому договорі, укладеному між сторонами.

(f) У разі виникнення суперечності між СДП ЄС та цими Положеннями, переважну силу матимуть СДП ЄС.

5.3 Стосовно Доповнення(-нь) СК:

(a) Якщо Постачальник не зареєстрований у Країні з належним рівнем захисту: (i) Постачальник цим укладає Доповнення СК з компанією Kyndryl у якості Імпортера на додаток до СДП ЄС, зазначених вище (якщо застосовно, залежно від обставин опрацювання); та (ii) Постачальник укладе письмові договори з кожним затвердженим Суброзпорядником та надасть Kyndryl копії цих договорів за запитом.

(b) Якщо Постачальник зареєстрований у Країні з належним рівнем захисту, а компанія Kyndryl є Володільцем, який не підпадає під дію Загального регламенту СК про захист даних (відповідно до законодавства Сполученого Королівства відповідно до Закону про вихід з Європейського Союзу 2018 р.), Постачальник цим укладає Доповнення СК з Kyndryl у якості Експортера для додавання до СДП ЄС, викладених у Розділі 5.2 (b) вище.

(c) Якщо Інші Володільці, такі як Замовники або афілійовані особи, вимагають приєднання до Доповнення(-нь) СК, Постачальник цим погоджується з будь-якою такою вимогою.

(d) Додаток з інформацією (як зазначено в Таблиці 3) у Доповненні(-ях) СК можна знайти в застосовних СДП ЄС, цих Положеннях, самому Транзакційному документі та пов'язаному базовому договорі між сторонами. Ні Kyndryl, ні Постачальник не можуть розірвати Доповнення СК у разі внесення до нього змін.

(e) У разі виникнення суперечності між Доповненням(-и) СК та цими Положеннями переважну силу матиме Доповнення СК.

5.4 Щодо СДП Сербії:

(a) Якщо Постачальник зареєстрований не в Країні з належним рівнем захисту: (i) Постачальник цим укладає СДП Сербії із Kyndryl від імені самого Постачальника як Розпорядника; і (ii) Постачальник повинен укласти письмові договори з кожним затвердженим Суброзпорядником відповідно до пункту 8 СДП Сербії і надати Kyndryl копії таких договорів на запит Kyndryl.

(b) Якщо Постачальник зареєстрований у Країні з належним рівнем захисту, Постачальник цим укладає СДП Сербії з компанією Kyndryl від імені усіх Суброзпорядників, які знаходяться в Країнах з неналежним рівнем захисту. Якщо Постачальник не може це зробити від імені будь-якого з таких Суброзпорядників, Постачальник надасть Kyndryl підписані таким Суброзпорядником СДП Сербії для підписання Kyndryl, перш ніж дозволити Суброзпоряднику здійснювати Обробку будь-яких Персональних Даних Kyndryl.

(c) СДП Сербії, укладені між Kyndryl і Постачальником, виступатимуть або в якості СДП Сербії між Володільцем і Розпорядником, або в якості взаємної письмової угоди між «володільцем» і «розпорядником», залежно від обставин. У разі виникнення суперечностей між СДП Сербії та цими Положеннями, переважну силу матимуть СДП Сербії.

(d) Інформацію, яка є необхідною для заповнення Доповнень 1–8 до СДП Сербії з метою керування передачею Персональних Даних до країни, що не належить до Країн з належним рівнем

захисту, можна знайти в цих Положеннях та Додатку до Транзакційного Документа або в самому Транзакційному Документі.

5.5. Стосовно доповнення(-нь) Швейцарії:

(a) Якщо передача Персональних даних компанії Kyndryl відповідно до розділу 5.1. підпадає під дію Федерального закону Швейцарії про захист даних («FADP»), то регулювати таку передачу будуть СДП ЄС, узгоджені в розділі 5.2. цих Положень із наступними поправками з метою застосування Загального регламенту про захист даних («GDPR») для Персональних даних Швейцарії:

- Посилання на Загальний регламент про захист даних («GDPR») слід розуміти також як посилання на рівнозначні положення Федерального закону FADP,
- Швейцарська федеральна комісія з захисту даних та інформації є компетентним наглядовим органом у розумінні Пункту 13 СДП ЄС та Доповнення I.C до СДП ЄС
- У випадку, якщо передача підпадає виключно під дію Федерального закону FADP, така передача буде регулюватися законодавством Швейцарії.
- Термін «держава-член» з Пункту 18 СДП ЄС поширюється на Швейцарію з метою надання суб'єктам даних зі Швейцарії можливості відстоювати свої права за місцем свого постійного проживання.

(b) Для уникнення сумнівів жодне з вищенаведених положень не має метою жодним чином знизити рівень захисту даних, який забезпечується згідно зі СДП ЄС, їх мета — виключно поширення цього рівня захисту на суб'єктів даних у Швейцарії. В інших випадках та тією мірою, у якій це застереження не виконується, переважну силу матимуть СДП ЄС.

6. Сприяння та Ведення Обліку

6.1 З огляду на характер Обробки Постачальник зобов’язаний надавати Kyndryl допомогу в запровадженні належних технічних і організаційних заходів для виконання зобов’язань, пов’язаних із запитами та правами Суб’єктів Даних. Постачальник зобов'язаний також сприяти Kyndryl із метою забезпечення дотримання зобов'язань у зв'язку з безпекою Обробки, повідомленням та інформуванням про Порушення Безпеки і проведенням оцінки потенційного впливу на захист даних,включно з попередньою консультацією з відповідальним регуляторним органом, якщо це вимагається, зважаючи на інформацію, доступну Постачальнику.

6.2 Постачальник зобов'язаний вести облік імен/назв і контактних даних кожного Суброзпорядника, включаючи кожного представника Суброзпорядника та кожної особи, відповідальної за захист даних. Постачальник зобов'язаний надавати такі облікові записи на вимогу Kyndryl у строки, які дозволять Kyndryl своєчасно відповісти на будь-який запит Замовника або третьої особи.

Стаття IV. Технічні та організаційні заходи, Захист коду

Ця Стаття застосовується, якщо Постачальник має доступ до Вихідного Коду Kyndryl. Постачальник зобов'язаний дотримуватись вимог цієї Статті і таким чином захищати Вихідний Код Kyndryl від втрати, знищення, зміни, випадкового або несанкціонованого розкриття, випадкового або несанкціонованого доступу та незаконних форм Взаємодії. Вимоги цієї Статті поширюються на всі прикладні програми, платформи та інфраструктуру IT, функціонування яких або управління якими забезпечує Постачальник під час надання Результатів і Послуг і під час Взаємодії з Технологіями Kyndryl, включаючи всі послуги розробки, тестування, розміщення, підтримки, експлуатації та середовища центрів обробки даних.

1. Вимоги щодо Безпеки

Нижченаведені терміни вживаються в такому значенні:

Заборонена країна: будь-яка країна: (a) яку уряд США визнав іноземним противником відповідно до Указу Президента США «Про гарантування безпеки постачань інформаційно-комунікаційних технологій і послуг» від 15 травня 2019 року, (b) яку внесено в список відповідно до розділу 1654 Закону США про бюджетні асигнування на національну оборону 2019 року або (c) яку визнано «Забороненою країною» в Документі Транзакції.

1.1 Постачальник зобов'язується не розповсюджувати та не депонувати будь-який Вихідний Код Kyndryl на користь будь-яких третіх осіб.

1.2 Постачальник зобов'язується не допускати розміщення Вихідного Коду Kyndryl на серверах, що знаходяться в Забороненій країні.Постачальник зобов'язується не допускати, щоб будь-як особи, включаючи його Персонал, які знаходяться або тимчасово перебувають у Забороненій країні (протягом усього часу свого перебування), з будь-якої причини, отримували доступ або використовували будь-який Вихідний Код Kyndryl, незалежно від того, в якій країні або регіоні світу знаходиться такий Вихідний код, і Постачальник зобов'язується не допускати здійснення будь-яких розробок, тестування чи інших послуг у Забороненій країні, що потребує такого доступу або використання.

1.3 Постачальник зобов'язується не розміщати або не розповсюджувати Вихідний Код Kyndryl у будь-якій юрисдикції, де законодавство або тлумачення законодавства вимагає розкриття Вихідного Коду будь-яким третім особам. Якщо в юрисдикції, де знаходиться Вихідний Код Kyndryl, змінюється законодавство або тлумачення законодавства, що може призвести до того, що Постачальник буде зобов'язаний розкрити такий Вихідний Код третім особам, Постачальник повинен негайно знищити або негайно вивести такий Вихідний Код Kyndryl з цієї юрисдикції, і не розміщати в ній будь-який додатковий Вихідний Код Kyndryl, допоки там діятиме таке законодавство або тлумачення законодавства.

1.4 Постачальник зобов'язується, прямо чи опосередковано, не вживати жодних дій, включаючи укладення будь-якої угоди, внаслідок яких Постачальник, Kyndryl або будь-яка третя особа буде зобов'язана розкрити інформацію згідно з розділами 1654 або 1655 Закону США про бюджетні асигнування на національну оборону 2019 року. Для ясності: Постачальнику за жодних обставин не дозволяється розкривати Вихідний Код Kyndryl будь-яким третім особам без попередньої письмової згоди Kyndryl, крім випадків, коли це прямо дозволено в Документі Транзакції або пов'язаному базовому договорі між сторонами.

1.5 Якщо Kyndryl повідомить Постачальника або якщо третя особа повідомить будь-яку зі сторін про те, що: (a) Постачальник дозволив перенести Вихідний Код Kyndryl у Заборонену країну або будь-яку юрисдикцію, що підпадає під дію розділу 1.3 вище, (b) Постачальник іншим чином випустив Вихідний Код Kyndryl, отримав доступ до нього або використав його способом, не дозволеним Документом Транзакції або пов'язаним базовим або іншим договором між сторонами, або (c) Постачальник порушив розділ 1.4 вище, тоді без обмеження прав Kyndryl вжити заходів для усунення такого порушення за законодавством, або за правом справедливості, або згідно з Документом Транзакції, або пов'язаним базовим або іншим договором між сторонами: (i) якщо таке повідомлення

надійде до Постачальника, Постачальник негайно передасть це повідомлення Kyndryl; і (ii) Постачальник, відповідно до вмотивованих розпоряджень Kyndryl, розслідує та усуне порушення в строки, обґрунтовано встановлені Kyndryl (після консультації з Постачальником).

1.6 Якщо Kyndryl обґрунтовано вважатиме, що зміни в політиці, процедурах, засобах контролю або практиках Постачальника щодо доступу до Вихідного Коду можуть бути необхідними для усунення ризиків кібербезпеки, крадіжки інтелектуальної власності або подібних або пов'язаних із ними ризиків (включаючи ризик того, що без таких змін Kyndryl може бути обмежена в питаннях продажу певним Замовникам, або на певних ринках або іншим чином не зможе задовольнити вимоги Замовника щодо вимог безпеки або постачання), тоді Kyndryl може зв'язатися з Постачальником і обговорити дії, необхідні для усунення таких ризиків, включаючи зміни до таких політик, процедур, засобів контролю чи практик. За запитом Kyndryl Постачальник співпрацюватиме з Kyndryl, щоб разом оцінити, чи потрібні такі зміни, і запровадити відповідні взаємоузгоджені зміни.

Стаття V. Безпечна розробка

Ця Стаття застосовується, якщо Постачальник надаватиме Kyndryl свій Вихідний Код або Вихідний Код сторонніх виробників або Локальне Програмне забезпечення, або якщо будь-які Результати чи Послуги Постачальника надаватимуться Замовнику Kyndryl у складі продукту або послуги Kyndryl.

1. Належний рівень безпеки

1.1 Постачальник підключиться до внутрішніх процесів Kyndryl, за допомогою яких оцінюється належний рівень безпеки продуктів і послуг Kyndryl, що залежать від Результатів Постачальника, у тому числі шляхом своєчасного та повного реагування на запити про отримання інформації шляхом надання документів, інших реєстраційних записів, проведення опитування відповідного Персоналу Постачальника тощо.

2. Безпечна розробка

2.1 Цей розділ 2 застосовується лише тоді, коли Постачальник надає Kyndryl Локальне Програмне Забезпечення.

2.2 Постачальник запровадив і підтримуватиме протягом усього строку дії Транзакційного Документа, відповідно до Кращих Практик Індустрії, мережу, платформу, систему, прикладну програму, пристрій, фізичну інфраструктуру, систему реагуванням на інциденти, а також орієнтовані на Персонал політики безпеки, процедури та засоби контролю, які є необхідними для захисту: (a) систем і середовищ розробки, компонування, тестування та експлуатації, які Постачальник або будь-яка третя особа, залучена Постачальником, експлуатує, контролює, використовує або іншим чином застосовує у зв’язку з Результатами, і (b) всього вихідного коду Результатів від втрати, незаконних форм обробки та несанкціонованого доступу, розкриття або зміни.

3. Сертифікація відповідності вимогам стандарту ISO 20243

3.1 Цей розділ 3 застосовується лише тоді, коли будь-які Результати або Послуги Постачальника надаватимуться Замовнику Kyndryl у складі продукту або послуги Kyndryl.

3.2 Постачальник отримає сертифікат відповідності вимогам стандарту ISO 20243 «Інформаційні технології. Відкритий стандарт на довірених постачальників технологій. Мінімізація ризику залучення у виробничий процес зловмисно зіпсованих і контрафактних компонентів» (Information technology, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products) (сертифікація на основі самостійної оцінки або на основі оцінки авторитетного незалежного аудитора). У якості альтернативи, у разі подання Постачальником письмового запиту та отримання письмового схвалення Kyndryl, Постачальник отримає сертифікат відповідності вимогам

еквівалентного в істотній частині галузевого стандарту, який визначає практики безпечної розробки та постачання (сертифікація на основі самостійної оцінки або на основі оцінки авторитетного незалежного аудитора, за умови та після схвалення Kyndryl).

3.3 Постачальник отримає сертифікат відповідності стандарту ISO 20243 або сертифікат еквівалентного йому в істотній частині галузевого стандарту (за умови письмового схвалення Kyndryl) протягом 180 днів після дати набуття Документом Транзакції чинності
і далі поновлюватиме сертифікат кожні 12 місяців після цього (відповідно до чинної на той момент найпізнішої версії застосовного стандарту, тобто ISO 20243 або, за умови письмового схвалення Kyndryl, еквівалентного йому в істотній частині галузевого стандарту, який визначає практики безпечної розробки та постачання).

3.4 Постачальник, за запитом, негайно надає Kyndryl копію сертифікатів, які Постачальник зобов'язаний отримати відповідно до розділів 2.1 і 2.2 вище.

4. Вразливості Безпеки

Нижченаведені терміни вживаються в такому значенні:

Виправлення помилок: виправлення несправностей і зміни, які виправляють помилки або недоліки, включаючи Вразливості Безпеки, в Результатах.

Зменшення Ризику: усі відомі засоби, призначені для зменшення або уникнення ризиків, пов'язаних із Вразливістю Безпеки.

Вразливість Безпеки: стан у проектуванні, кодуванні, розробці, реалізації, тестуванні, експлуатації, підтримці, обслуговуванні або керуванні Результатом, який дозволяє будь-кому здійснити атаку, що може призвести до несанкціонованого доступу або використання, включаючи (a) здійснення доступу, отримання контролю або порушення роботи системи, (b) здійснення доступу, видалення, змінення або вилучення даних або (c) змін ідентифікаційних даних, авторизацій або прав доступу користувачів або адміністраторів. Вразливість Безпеки може існувати незалежно від того, чи призначено їй ID CVE (Загальновідомі вразливості інформаційної безпеки) або будь-який рейтинг чи офіційний класифікатор.

4.1 Постачальник заявляє й гарантує, що він буде: (a) використовувати Кращі Практики індустрії для виявлення Вразливостей Безпеки, зокрема шляхом безперервного статичного та динамічного сканування безпеки вихідного коду прикладних програм, сканування безпеки відкритого коду та сканування вразливостей безпеки, та (b) виконувати вимоги цих Положень із метою попередження, виявлення та виправлення Вразливостей Безпеки в Результатах та в усіх прикладних програмах, платформах та інфраструктурі IT, які Постачальник використовує для створення та надання Послуг і Результатів.

4.2 Якщо Постачальнику стане відомо про Вразливість Безпеки в Результатах або будь-якій такій прикладній програмі, платформі або інфраструктурі IT, Постачальник забезпечить Kyndryl Виправлення Помилок і Зменшення Ризику для всіх версій і випусків Результатів відповідно до наступних Рівнів Серйозності та строків:

Рівень Серйозності*
Аварійна Вразливість Безпеки: Вразливість Безпеки, яка становить серйозну та, ймовірно, глобальну загрозу. Kyndryl визначає Аварійну Вразливість Безпеки на власний розсуд, незалежно від Базової Оцінки CVSS.
Критична: Вразливість Безпеки, яка має Базову Оцінку CVSS від 9 до 10,0
Висока: Вразливість Безпеки, яка має Базову Оцінку CVSS від 7,0 до 8,9
Помірна: Вразливість Безпеки, яка має Базову Оцінку CVSS від 4,0 до 6,9
Низька: Вразливість Безпеки, яка має Базову Оцінку CVSS від 0,0 до 3,9

Строки				
Аварійна	***Критична***	***Висока***	***Помірна***	***Низька***
До 4 Днів, як визначено Головним управлінням інформаційної безпеки Kyndryl	30 Днів	30 Днів	90 Днів	Відповідно до Кращих практик індустрії

* У всіх випадках, коли Вразливості Безпеки ще не призначено Базову Оцінку CVSS, Постачальник застосовуватиме Рівень Серйозності, який відповідає характеру та обставинам такої вразливості.

4.3 Для Вразливості Безпеки, яка стала загальновідомою і для якої Постачальник ще не забезпечив Kyndryl Виправлення Помилки або Зменшення Ризику, Постачальник запровадить будь-які технічно можливі додаткові заходи безпеки, які можуть пом'якшити ризики цієї вразливості.

4.4 Якщо Kyndryl не задовольнить відповідь Постачальника на будь-яку Вразливість Безпеки в Результатах або будь-якій прикладній програмі, платформі або інфраструктурі, вказаній вище, тоді без обмеження будь-яких інших прав Kyndryl Постачальник негайно організує для Kyndryl обговорення зауважень із Віце-президентом Постачальника або особою, еквівалентною за посадою, яка відповідає за Виправлення Помилки.

4.5 Приклади Вразливостей Безпеки включають сторонній код або відкритий код, що не обслуговується (EOS), для яких не випускатимуться виправлення безпеки.

Стаття VI. Доступ до Корпоративних Систем

Ця Стаття застосовується, якщо працівники Постачальника матимуть доступ до будь-яких Корпоративних Систем.

1. Загальні положення

1.1 Kyndryl визначить, чи дозволяти працівникам Постачальника доступ до Корпоративних Систем. Якщо Kyndryl надасть такий дозвіл, Постачальник зобов'язується дотримуватися вимог цієї Статті і забезпечити дотримання таких вимог своїми працівниками, які отримають такий доступ.

1.2 Kyndryl визначить засоби, за допомогою яких працівники Постачальника можуть отримати доступ до Корпоративних Систем, зокрема, чи будуть такі працівники отримувати доступ до Корпоративних Систем за допомогою Пристроїв, що надаються Kyndryl або Постачальником.

1.3 Працівники Постачальника можуть отримувати доступ до Корпоративних Систем і використовувати Пристрої, дозволені Kyndryl для такого доступу, виключно для надання Послуг. Працівники Постачальника не можуть використовувати Пристрої, дозволені Kyndryl, для надання послуг будь-якій іншій особі або організації, або для отримання доступу до будь-яких IT-систем, мереж, програм, сайтів, інструментів електронної пошти, інструментів співпраці тощо, що належать Постачальнику або третім особам, для надання Послуг або у зв'язку з ними.

1.4 Для ясності: працівники Постачальника не можуть використовувати Пристрої, дозволені Kyndryl для доступу до Корпоративних Систем, в особистих цілях (наприклад, працівники Постачальника не можуть зберігати на таких Пристроях особисті файли, такі як музика, відео, світлини тощо, і не можуть користуватися інтернетом в особистих цілях за допомогою таких Пристроїв).

1.5 Працівники Постачальника не копіюватимуть Матеріали Kyndryl, доступні через Корпоративну Систему, без попереднього письмового дозволу Kyndryl (і за жодних обставин не копіюватимуть будь-які Матеріали Kyndryl на портативний пристрій зберігання даних, такий як USB-накопичувач, зовнішній жорсткий диск тощо).

1.6 За запитом Постачальник підтверджує, за іменем працівника, конкретні Корпоративні Системи, до яких його працівники мають право доступу і до яких вони зверталися протягом будь-якого періоду часу, визначеного Kyndryl.

1.7 Постачальник повідомляє Kyndryl протягом 24 (двадцяти чотирьох) годин після того, як будь-який працівник Постачальника, який має доступ до будь-якої Корпоративної Системи, більше не: (a) працює в компанії Постачальника або (b) виконує роботу, яка вимагає такого доступу. Постачальник співпрацюватиме з Kyndryl, щоб забезпечити негайне скасування доступу для таких колишніх або діючих працівників.

1.8 Постачальник негайно повідомлятиме Kyndryl про будь-які фактичні або ймовірні інциденти, пов'язані з порушенням безпеки (наприклад, про втрату Пристрою Kyndryl або Постачальника, несанкціонований доступ до Пристрою або даних, матеріалів чи іншої інформації будь-якого типу), і співпрацюватиме з Kyndryl у розслідуванні таких інцидентів.

1.9 Постачальник не повинен дозволяти будь-якому агенту, працівнику незалежного підрядника або субпідрядника отримувати доступ до будь-якої Корпоративної Системи без попередньої письмової згоди Kyndryl; якщо Kyndryl надасть таку згоду, Постачальник встановить для цих осіб та їхніх роботодавців договірні зобов'язання дотримуватися вимог цієї Статті так, наче ці особи є працівниками Постачальника, і відповідатиме перед Kyndryl за всі дії та бездіяльність таких осіб або роботодавців у зв'язку з таким доступом до Корпоративних Систем.

2. Програмне забезпечення Пристроїв

2.1 Постачальник направлятиме своїх працівників, щоб вони своєчасно встановили все програмне забезпечення Пристроїв, яке необхідне Kyndryl для організації безпечного доступу до Корпоративних Систем. Ані Постачальник, ані його працівники не втручатимуться в роботу цього програмного забезпечення або захисних функцій, які надає програмне забезпечення.

2.2 Постачальник та його працівники дотримуватимуться правил налаштування Пристрою, які встановлює Kyndryl, а інакше співпрацюватимуть з Kyndryl, щоб забезпечити функціонування програмного забезпечення так, як потрібно Kyndryl. Наприклад, Постачальник не перевизначатиме функції програмного забезпечення щодо блокування сайтів чи автоматичних функцій виправлення.

2.3 Працівники Постачальника не можуть передавати Пристрої, якими вони користуються для доступу до Корпоративних Систем, або імена користувачів, паролі тощо до своїх Пристроїв будь-яким іншим особам.

2.4 Якщо Kyndryl уповноважує працівників Постачальника отримувати доступ до Корпоративних Систем за допомогою Пристроїв Постачальника, Постачальник встановить та запустить операційну систему на тих Пристроях, які схвалить Kyndryl, та оновить її до нової версії або нової операційної системи протягом обґрунтовано необхідного часу після отримання таких вказівок від Kyndryl.

3. Контроль і Співпраця

3.1 Kyndryl має необмежені права контролювати та усувати наслідки можливих вторгнень та інших загроз кібербезпеки будь-якими способами, з будь-якого місця та використовуючи будь-які засоби, які, на думку Kyndryl, є необхідними або доречними, без попереднього повідомлення Постачальника, будь-якого працівника Постачальника чи інших осіб. Наприклад, Kyndryl може в будь-який час (a) провести перевірку безпеки на будь-якому Пристрої, (b) контролювати, відновлювати за допомогою технічних чи інших засобів і переглядати повідомлення (включаючи електронні листи з будь-яких облікових записів електронної пошти), записи, файли тощо, які зберігаються на будь-якому Пристрої або передаються через будь-яку Корпоративну Систему, та (c) отримувати повне відображення для експертного аналізу будь-якого Пристрою. Якщо у Kyndryl виникне необхідність у співпраці з Постачальником для реалізації своїх прав, Постачальник буде повністю та своєчасно виконувати запити Kyndryl щодо такої співпраці (включаючи, наприклад, запити щодо безпечного налаштування будь-якого Пристрою, встановлення засобів спостереження чи іншого програмного забезпечення на будь-якому Пристрої, обміну даними про з'єднання на рівні системи, участі в заходах реагування на інциденти на будь-якому Пристрої та надання фізичного доступу до будь-якого Пристрою для отримання Kyndryl повного відображення для експертного аналізу або для інших цілей, а також подібні та пов'язані з ними запити).

3.2 Kyndryl може в будь-який час скасувати доступ будь-якого працівника Постачальника або всіх працівників Постачальника до Корпоративних Систем без попереднього повідомлення Постачальника, будь-якого працівника Постачальника або інших осіб, якщо Kyndryl вважатиме це необхідним для захисту Kyndryl.

3.3 Права Kyndryl не припиняються, не зменшуються і жодним чином не обмежуються будь-яким положенням Документа Транзакції, пов'язаного базового договору або будь-якого іншого договору між сторонами, включаючи будь-яке положення, яке може зобов'язувати зберігати дані, матеріали чи іншу інформацію будь-якого типу лише у певному місці чи місцях або містити умову, щоб доступ до таких даних, матеріалів чи іншої інформації був дозволений лише особам із певного місця чи місць.

4. Пристрої Kyndryl

4.1 Kyndryl зберігає за собою право власності на всі Пристрої Kyndryl, а Постачальник несе відповідальність за втрату Пристроїв, у тому числі через крадіжку, умисне знищення або пошкодження

або недбалість. Постачальник не буде і не дозволятиме іншим вносити будь-які зміни в Пристрої Kyndryl без попередньої письмової згоди Kyndryl; під змінами розуміють будь-які зміни в Пристрої, включаючи будь-які зміни в програмному забезпеченні Пристрою, прикладних програмах, проекті безпеки, конфігурації безпеки або фізичної, механічної та електричної конфігурації.

4.2 Постачальник зобов'язаний повернути всі Пристрої Kyndryl протягом 5 робочих днів після того, як зникне потреба в цих Пристроях для надання Послуг, і на вимогу Kyndryl — одночасно знищити всі дані, матеріали та іншу інформацію будь-якого типу на цих Пристроях, не залишаючи собі жодної копії; при цьому Постачальник повинен дотримуватися Кращих Практик індустрії, щоб видалити усі такі дані, матеріали та іншу інформацію без можливості їхнього відновлення. Постачальник зобов'язаний запакувати та повернути Пристрої Kyndryl у тому самому стані, в якому вони були передані Постачальнику, з урахуванням природного зношування, за власний рахунок у місці, визначеному Kyndryl. Невиконання Постачальником будь-яких зобов'язань, передбачених у цьому розділі 4.2, є істотним порушенням Документа Транзакції, відповідного базового договору та будь-якого пов'язаного договору між сторонами; при цьому договір є «пов'язаним», якщо доступ до будь-якої Корпоративної Системи полегшує завдання або іншу діяльність Постачальника за цим договором.

4.3 Kyndryl надаватиме підтримку Пристроїв Kyndryl (включаючи перевірку Пристроїв, а також профілактичне та ремонтне обслуговування). Постачальник зобов'язаний негайно повідомляти Kyndryl про необхідність ремонтного обслуговування.

4.4. Для програм програмного забезпечення, які належать Kyndryl або на які Kyndryl має право надавати ліцензії, Kyndryl надає Постачальнику тимчасове право використовувати, зберігати та робити достатню кількість копій, які будуть потрібні йому для дозволеного використання Пристроїв Kyndryl. Постачальник не може передавати програми кому-небудь, робити копії інформації про ліцензію на програмне забезпечення, а також розбирати, декомпілювати, виконувати інженерний аналіз або іншим чином транслювати будь-яку програму, якщо це прямо не дозволено чинним законодавством, без права на відмову від виконання договірних зобов'язань.

5. Оновлення

5.1 Незважаючи на положення про інше, які містяться в Документі Транзакції або пов'язаному базовому договорі між сторонами, після письмового повідомлення Постачальника та без необхідності отримувати згоду Постачальника, Kyndryl може оновити, доповнити або іншим чином змінити цю Статтю з урахуванням будь-яких вимог чинного законодавства або зобов'язань Замовника з метою підтримки актуальності кращих практик у галузі безпеки або з інших причин, як Kyndryl вважатиме за необхідне для захисту Корпоративних Систем або Kyndryl.

Стаття VII. Доповнення штату

Ця Стаття застосовується, якщо працівники Постачальника надаватимуть Послуги від імені Kyndryl протягом повного робочого дня, працюючи з приміщень Kyndryl, приміщень Постачальника або зі свого дому, і під час надання Послуг користуватимуться для доступу до Корпоративних Систем виключно Пристроями Kyndryl.

1. Доступ до Корпоративних Систем; Середовища Kyndryl

1.1 Для надання Послуг Постачальник має отримувати доступ до Корпоративних Систем виключно за допомогою Пристроїв, які надає Kyndryl.

1.2 При здійсненні доступу до Корпоративних Систем Постачальник зобов'язується дотримуватися умов, викладених у Статті VI (Доступ до Корпоративних Систем).

1.3 Єдиними Пристроями, якими дозволяється користуватися Постачальнику та його працівникам для надання Послуг, є Пристрої, що надаються Kyndryl; такі Пристрої дозволяється використовувати тільки для надання Послуг. Для ясності: за жодних обставин Постачальник або його працівники не можуть використовувати будь-які інші пристрої для надання Послуг або використовувати Пристрої Kyndryl для будь-якого іншого замовника Постачальника або з будь-якою метою, окрім надання Послуг Kyndryl.

1.4 Працівники Постачальника, які використовують Пристрої Kyndryl, можуть обмінюватися Матеріалами Kyndryl між собою та зберігати такі матеріали на Пристроях Kyndryl, але лише в тому обсязі, в якому такий обмін і зберігання необхідні для успішного надання Послуг.

1.5 За винятком такого зберігання на Пристроях Kyndryl, Постачальник або його працівники за жодних обставин не можуть вилучати будь-які Матеріали Kyndryl зі сховищ Kyndryl, середовищ, інструментів або інфраструктури, де вони зберігаються Kyndryl.

1.6 Для ясності: Постачальник та його працівники не мають права передавати будь-які Матеріали Kyndryl до будь-яких сховищ, середовищ, інструментів чи інфраструктури Постачальника або будь-яких інших систем, платформ, мереж Постачальника тощо, без попередньої письмової згоди Kyndryl.

1.7 Стаття VIII (Технічні та організаційні заходи, Загальні параметри безпеки) не застосовується до Послуг Постачальника, якщо працівники Постачальника надаватимуть Послуги Kyndryl протягом усього їх робочого часу, працюючи з приміщень Kyndryl, приміщень Постачальника або зі свого дому, і під час надання Послуг користуватимуться для доступу до Корпоративних Систем виключно Пристроями Kyndryl. В іншому випадку до Послуг Постачальника застосовується Стаття VIII.

Стаття VIII. Технічні та організаційні заходи, Загальні параметри безпеки

Ця Стаття застосовується, якщо Постачальник надає Kyndryl будь-які Послуги або Результати, за винятком ситуацій, коли Постачальник надає доступ лише до ВСІ Kyndryl у процесі надання таких Послуг і Результатів (наприклад, Постачальник не Оброблятиме будь-які інші Дані Kyndryl і не матиме доступу до будь-яких інших Матеріалів Kyndryl або до будь-якої Корпоративної Системи), єдиними Послугами та Результатами Постачальника є надання Kyndryl Локального Програмного Забезпечення, або Постачальник надає всі свої Послуги та Результати на основі моделі доповнення штату відповідно до Статті VII, включно з розділом 1.7.

Постачальник зобов'язаний дотримуватися вимог цієї Статті і таким чином захищати: (a) Матеріали Kyndryl від втрати, знищення, зміни, випадкового або несанкціонованого розкриття, випадкового або несанкціонованого доступу, (b) Дані Kyndryl від незаконних форм Обробки і (c) Технології Kyndryl від незаконних форм Взаємодії. Вимоги цієї Статті поширюються на всі прикладні програми, платформи та інфраструктуру IT, функціонування яких або управління якими забезпечує Постачальник під час надання Результатів і Послуг і під час Взаємодії з Технологіями Kyndryl, включаючи всі послуги розробки, тестування, розміщення, підтримки, експлуатації та середовища центрів обробки даних.

1. Політики Безпеки

1.1 Постачальник зобов'язаний актуалізувати та дотримуватися політик і практик у галузі IT-безпеки, які є невід'ємною частиною діяльності Постачальника та є обов'язковими для всього Персоналу Постачальника, відповідно до Кращих Практик індустрії.

1.2 Постачальник зобов'язаний переглядати свої політики та практики у галузі IT-безпеки принаймні один раз на рік і вносити в них зміни, які Постачальник вважатиме за потрібне для забезпечення захисту Матеріалів Kyndryl.

1.3 Постачальник зобов'язаний дотримуватись стандартних обов'язкових вимог щодо перевірки працевлаштування всіх нових найманих працівників, актуалізувати їх та поширювати такі вимоги на весь Персонал Постачальника та дочірні компанії, що перебувають у повному розпорядженні Постачальника. Ці вимоги будуть містити перевірки кримінального минулого в обсягах, дозволених місцевим законодавством, підтвердження ідентифікаційних даних та будь-які додаткові перевірки, які Постачальник вважатиме необхідними. Постачальник проводитиме періодичні перевірки виконання цих вимог, які він вважатиме необхідними.

1.4 Постачальник зобов'язаний щорічно організовувати навчання своїх працівників у галузі безпеки та конфіденційності та вимагати від усіх таких працівників щорічно підтверджувати дотримання принципів етичної поведінки, конфіденційності та політик безпеки Постачальника, як це зазначено в кодексі етичної поведінки Постачальника або аналогічних документах. Постачальник зобов'язаний забезпечити додаткове навчання щодо політик і процесів для осіб із адміністративними правами доступу до будь-яких компонентів Послуг, Результатів або Матеріалів Kyndryl, спеціально призначене відповідно до їхніх службових обов'язків і підтримки Послуг, Результатів або Матеріалів Kyndryl, а також у разі необхідності забезпечити відповідність вимогам і сертифікацію.

1.5 Постачальник зобов'язаний спроектувати заходи з безпеки та конфіденційності для захисту та забезпечення доступності Матеріалів Kyndryl, зокрема шляхом впровадження, підтримки та забезпечення відповідності політикам і процедурам, які вимагають проектованої безпеки та конфіденційності, захисту техніки, а також захисту операцій, для всіх Послуг і Результатів, а також для Взаємодії з Технологіями Kyndryl.

2. Інциденти Безпеки

2.1 Постачальник зобов'язаний дотримуватися задокументованих політик реагування на інциденти безпеки та актуалізувати їх відповідно до Кращих Практик індустрії щодо обробки інцидентів, пов'язаних із безпекою комп'ютерів.

2.2 Постачальник зобов'язаний проводити розслідування випадків несанкціонованого доступу до Матеріалів Kyndryl або несанкціонованого використання Матеріалів Kyndryl, а також визначити і виконати відповідний план реагування.

2.3 Постачальник зобов'язаний невідкладно (але в жодному разі не пізніше ніж протягом 48 годин) повідомити Kyndryl, щойно йому стане відомо про будь-яке Порушення Безпеки. Постачальник надаватиме таке повідомлення за адресою cyber.incidents@kyndryl.com.Постачальник зобов'язаний надати на обґрунтований запит Kyndryl інформацію щодо такого порушення та будь-яких дій Постачальника, спрямованих на виправлення та відновлення діяльності. Наприклад, обґрунтовано запитувана інформація може включати журнали, що підтверджують доступ привілейованих користувачів, адміністраторів та інших користувачів до Пристроїв, систем або прикладних програм, образів для експертного аналізу Пристроїв, систем або прикладних програм та інші подібні елементи, наскільки вони стосуються порушення або його виправлення Постачальником і відновлення діяльності.

2.4 Постачальник зобов'язаний належним чином сприяти виконанню Kyndryl зобов'язань, передбачених законодавством (зокрема зобов'язань з інформування регуляторних органів або Суб'єктів Даних) Kyndryl, афілійованих осіб Kyndryl і Замовників (а також їхніх афілійованих осіб і замовників) у зв'язку з Порушенням Безпеки.

2.5 Постачальник зобов’язаний не інформувати й не сповіщати будь-яких третіх осіб про те, що Порушення безпеки прямо чи опосередковано стосується Kyndryl або Матеріалів Kyndryl, окрім випадків, коли Kyndryl дасть письмовий дозвіл на це або це вимагається законодавством. Постачальник зобов’язаний письмово повідомити Kyndryl перед розповсюдженням передбачених законодавством повідомлень для третіх осіб, якщо такі повідомлення прямо чи опосередковано розкриватимуть ідентифікаційну інформацію Kyndryl.

2.6 У разі Порушення Безпеки, яке виникло внаслідок порушення Постачальником будь-якого зобов'язання за цими Положеннями:

(a) Постачальник несе відповідальність за усі понесені ним витрати, а також за фактичні витрати, понесені Kyndryl, у зв'язку з повідомленням про Порушення Безпеки відповідним регуляторним органам, іншим державним органам і галузевим органам самоврядування, засобам масової інформації (якщо цього вимагає застосовне законодавство) і Суб'єктам Даних, Замовникам та іншим особам;

(b) на запит Kyndryl Постачальник зобов'язаний організувати і підтримувати за власні кошти кол-центр для відповідей на запитання Суб'єктів Даних щодо Порушення Безпеки та його наслідків протягом 1 року після дати, коли такі Суб'єкти Даних отримали повідомлення про Порушення Безпеки, або в порядку, передбаченому будь-яким застосовним законодавством про захист даних, залежно від того, що забезпечить надійніший захист. Kyndryl і Постачальник працюватимуть разом для створення сценаріїв та інших матеріалів для використання персоналом кол-центру під час обробки запитів. Крім того, повідомивши Постачальника письмово, Kyndryl може організувати та підтримувати власний кол-центр, замість зобов'язування Постачальника створювати кол-центр; Постачальник повинен відшкодувати Kyndryl фактичні витрати, понесені Kyndryl при створенні та підтримці такого кол-центру; і

(c) Постачальник зобов'язаний відшкодувати Kyndryl фактичні витрати, пов'язані з наданням послуг моніторингу компенсацій і відновлення компенсацій, протягом 1 року після дати повідомлення про Порушення Безпеки всіх осіб, яких стосується порушення і які зареєструвалися для отримання таких послуг, або в порядку, передбаченому будь-яким застосовним законодавством про захист даних, залежно від того, що забезпечить надійніший захист.

3. Фізичний Захист і Вхідний Контроль (далі термін «Об'єкт» означає фізичну локацію, де Постачальник розміщує, обробляє або іншим чином отримує доступ до Матеріалів Kyndryl).

3.1 Постачальник зобов'язаний забезпечити належний фізичний вхідний контроль, наприклад загородження, пункти входу з доступом по картках, камери спостереження та служби реєстрації відвідувачів, для захисту від несанкціонованого входу на Об'єкти.

3.2 Постачальник вимагатиме авторизації для доступу на Об'єкти та до контрольованих дільниць на Об'єктах, у тому числі будь-якого тимчасового доступу, а також обмежуватиме доступ відповідно до

посади працівника і службової необхідності. Якщо Постачальник надає тимчасовий доступ, його вповноважений працівник супроводжуватиме будь-якого такого відвідувача під час перебування на Об'єкті та в будь-яких контрольованих дільницях.

3.3 Постачальник запровадить засоби контролю фізичного доступу, зокрема засоби контролю доступу на основі багатофакторної автентифікації, які відповідають Кращим Практикам індустрії, щоб належним чином обмежити вхід до контрольованих дільниць на Об'єктах, реєструватиме усі спроби входу та зберігатиме такі журнали щонайменше протягом одного року.

3.4 Постачальник зобов'язаний відкликати доступ на Об'єкти та на контрольовані дільниці на Об'єктах у разі (a) відсторонення уповноваженого працівника Постачальника з будь-яких причин або (b) зникнення в уповноваженого працівника Постачальника ділової потреби в такому доступі. Постачальник зобов'язаний дотримуватися офіційних задокументованих процедур відсторонення працівника, які включають швидке видалення зі списків контролю доступу та здавання пропусків доступу.

3.5 Постачальник зобов'язаний вживати запобіжних заходів для захисту фізичної інфраструктури, яка використовується для підтримки Послуг і Результатів, а також Взаємодії з Технологіями Kyndryl, від екологічних загроз, як природного, так і техногенного характеру, наприклад підвищення температури довкілля, пожежі, повені, вологості, крадіжки та вандалізму.

4. Контроль Доступу, Втручання, Передавання та Розподілу Обов'язків

4.1 Постачальник зобов'язаний підтримувати задокументовану архітектуру мережевої безпеки, яка використовується під час функціонування Послуг, надання ним Результатів і Взаємодії з Технологіями Kyndryl. Постачальник зобов'язаний окремо перевірити таку мережеву архітектуру та запровадити заходи, спрямовані на запобігання неавторизованим мережевим з'єднанням до систем, прикладних програм і мережевих пристроїв, для забезпечення дотримання вимог безпечної сегментації, ізоляції та стандартів захисту. Постачальник не може використовувати технологію бездротового зв'язку для розміщення та функціонування будь-яких Послуг, розміщених на сервері; в інших випадках Постачальник може використовувати бездротові мережеві технології для надання Послуг і Результатів, а також Взаємодії з Технологіями Kyndryl, але Постачальник повинен використовувати шифрування та забезпечити захищені механізми автентифікації для будь-яких таких бездротових мереж.

4.2 Постачальник зобов'язаний підтримувати заходи, розроблені для логічного відокремлення Матеріалів Kyndryl та запобігання розголошенню або несанкціонованому доступу до Матеріалів Kyndryl з боку неуповноважених осіб. Крім того, Постачальник зобов'язаний забезпечити відповідну ізоляцію робочих, неробочих та інших середовищ, і якщо Матеріали Kyndryl уже знаходяться в неробочому середовищі або передаються в таке середовище (наприклад, для відтворення помилки), Постачальник зобов'язаний гарантувати, що заходи безпеки та конфіденційності в неробочому середовищі відповідають аналогічним заходам у робочому середовищі.

4.3 Постачальник шифруватиме Матеріали Kyndryl під час передачі та зберігання (окрім випадків, коли Постачальник може надати Kyndryl достатні докази технічної неможливості шифрування Матеріалів Kyndryl під час зберігання). Крім того, Постачальник шифруватиме всі фізичні носії, якщо такі є, наприклад носії з файлами резервних копій. Постачальник зобов'язаний підтримувати задокументовані процедури безпечної генерації, видавання, розсилання, зберігання, заміни, відкликання, відновлення, резервування, знищення, отримання та використання ключів, пов'язаних із шифруванням даних. Постачальник зобов'язаний забезпечити відповідність криптографічних методів, які використовуються для шифрування, Кращим Практикам індустрії (таким як,наприклад, NIST SP 800-131a).

4.4 Якщо Постачальнику буде потрібен доступ до Матеріалів Kyndryl, Постачальник зобов'язаний обмежити такий доступ до мінімального рівня, необхідного для надання та підтримки Послуг і Результатів. Постачальник зобов'язаний забезпечити, щоб такий доступ, включно з адміністративним доступом до будь-яких основних компонентів (тобто привілейований доступ), був індивідуальним, таким, що ґрунтується на ролі, та вимагати затвердження й регулярної перевірки уповноваженими особами Постачальника відповідно до принципів розділення обов'язків. Постачальник зобов'язаний підтримувати заходи для ідентифікації та видалення зайвих і неактивних облікових записів.

Постачальник зобов'язаний анулювати облікові записи з привілейованим доступом протягом 24 (двадцяти чотирьох) годин після відсторонення власника облікового запису або на вимогу Kyndryl або будь-якого уповноваженого працівника Постачальника, наприклад менеджера власника облікового запису.

4.5 Відповідно до Кращих Практик індустрії, Постачальник зобов'язаний підтримувати технічні заходи, що забезпечують тайм-аути неактивних сеансів, блокування облікових записів після кількох послідовних невдалих спроб входу, надійної автентифікації на основі пароля або парольної фрази, а також заходи, що вимагають безпечної передачі та зберігання таких паролів і парольних фраз. Крім того, Постачальник застосовуватиме багатофакторну автентифікацію для привілейованого доступу до будь-яких Матеріалів Kyndryl без використання консолі.

4.6 Постачальник зобов'язаний відстежувати застосування прав привілейованого доступу та забезпечувати заходи керування подіями та інформацією про безпеку, призначені для: (a) виявлення спроб несанкціонованого доступу та діяльності; (b) сприяння своєчасному і відповідному реагуванню на такий доступ і діяльність; і (c) забезпечення аудиту відповідності задокументованим політикам Постачальника з боку Постачальника, Kyndryl (відповідно до її прав перевірки згідно з цими Положеннями та прав на аудит, визначених в Документі Транзакції, відповідному базовому договорі або іншому пов'язаному договоріміж сторонами) та інших осіб.

4.7 Постачальник зобов'язаний зберігати журнали реєстрації, відповідно до Кращих Практик індустрії, усіх операцій доступу адміністраторів, користувачів або іншого доступу чи операцій в системах або у зв'язку з системами, що використовуються для надання Послуг і Результатів, а також для Взаємодії з Технологіями Kyndryl (а також надавати такі журнали на запит Kyndryl). Постачальник зобов'язаний підтримувати заходи, спрямовані на захист від несанкціонованого доступу, модифікації та випадкового або навмисного знищення таких журналів.

4.8 Постачальник зобов'язаний забезпечити захист комп'ютерів для систем, які належать йому або якими він управляє, включаючи системи кінцевих користувачів, і які він використовує для надання Послуг або Результатів, або для Взаємодії з Технологіями Kyndryl; засоби захисту включають зокрема: брандмауери кінцевих точок, засоби шифрування всього диска, технології виявлення та протидії зловмисному коду та найновішим стійким загрозам в кінцевих точках на основі підписів та без використання підписів, рішення для тимчасового блокування екрану та керування кінцевими точками, що забезпечують виконання вимог щодо конфігурації безпеки та застосування виправлень. Крім того, Постачальник запровадить технічні та операційні засоби контролю, які забезпечать можливість доступу до мереж Постачальника лише з відомих та перевірених систем кінцевих користувачів.

4.9 Згідно з Кращими Практиками індустрії, Постачальник забезпечуватиме захист середовищ центрів обробки даних, де зберігаються або обробляються Матеріали Kyndryl, зокрема: засоби виявлення та попередження вторгнень та протидії атакам типу «відмова в обслуговуванні» та зниження їхніх ризиків.

5. Контроль Цілісності та Доступності Послуг і Систем

5.1 Постачальник зобов'язаний (a) проводити оцінку ризиків безпеки та конфіденційності принаймні один раз на рік; (b) проводити тестування безпеки та оцінювання вразливостей, включно з автоматичним скануванням безпеки системи та прикладних програм і неавтоматизованими процедурами етичного проникнення, перед застосуванням у робочому середовищі та щорічно після цього, що стосується Послуг і Результатів, а також щорічно у зв'язку із Взаємодією з Технологіями Kyndryl; (c) залучати кваліфіковану незалежну сторонню організацію для проведення тестування на проникнення згідно з Кращими Практиками індустрії принаймні раз на рік, причому тестування повинне включати як автоматичне, так і ручне тестування; (d) забезпечувати автоматизоване керування та перевірку кожного компонента Послуг і Результатів, а також у зв'язку із Взаємодією з Технологіями Kyndryl на відповідність вимогам конфігурації безпеки; і (e) виправляти виявлені вразливості або невідповідність вимогам конфігурації безпеки з урахуванням ризиків, імовірності використання та впливу. Постачальник зобов'язаний реалізувати обґрунтовані заходи, щоб уникнути порушення надання Послуг під час тестування, оцінювання, сканування та виправлення. На запит Kyndryl Постачальник надасть Kyndryl письмовий звіт про останні операції тестування на проникнення,

проведені Постачальником, який повинен містити принаймні найменування протестованих пропозицій, кількість систем або прикладних програм, обраних для тестування, дати тестування, методологію тестування та загальний огляд результатів.

5.2 Постачальник зобов'язаний підтримувати політики та процедури, призначені для управління ризиками, пов'язаними із застосуванням змін до Послуг або Результатів, або до Взаємодії з Технологіями Kyndryl. Перед застосуванням таких змін, включаючи зміни відповідних систем, мереж і базових компонентів, Постачальник зобов'язаний задокументувати в зареєстрованому запиті на зміну: (a) опис та причини зміни, (b) деталі реалізації та графік, (c) дані про ризики, що стосуються впливу на Послуги та Результати, замовників Послуг, або Матеріали Kyndryl, (d) очікуваний результат, (e) план відкликання та (f) процедуру затвердження уповноваженими працівниками Постачальника.

5.3 Постачальник зобов'язаний вести облік усіх IT-ресурсів, які використовуються під час надання Послуг, постачання Результатів і Взаємодії з Технологіями Kyndryl. Постачальник безперервно відстежуватиме та контролюватиме стан (у тому числі потужність) і доступність таких IT-ресурсів, Послуг, Результатів і Технологій Kyndryl, включаючи відповідні базові компоненти таких ресурсів, Послуг, Результатів і Технологій Kyndryl.

5.4 Постачальник розроблятиме всі системи, які він використовує в процесі розробки або функціонування Послуг і Результатів, а також під час Взаємодії з Технологіями Kyndryl, на основі попередньо визначених образів безпеки системи або рекомендацій безпеки, які відповідають Кращим Практикам індустрії, наприклад критеріям Центру інтернет-безпеки (CIS).

5.5 Без обмеження зобов'язань Постачальника або прав Kyndryl за Документом Транзакції або відповідним базовим договором міжсторонами стосовно безперервності бізнес-процесів Постачальник зобов'язаний окремо оцінювати кожну Послугу та Результат і кожну IT-систему, що використовується для Взаємодії з Технологіями Kyndryl, щодо виконання вимог безперервності бізнес-процесів та IT-процесів і відновлення в аварійних ситуаціях відповідно до задокументованих рекомендацій з управління ризиками. Постачальник зобов'язаний забезпечити, щоб кожна така Послуга, Результат та IT-система мала, у тій мірі, в якій це підтверджує оцінка ризиків, окремо визначені, задокументовані, підтримувані та щорічно перевірювані плани забезпечення безперервності бізнес-процесів та IT-процесів і програми аварійного відновлення згідно з Кращими практиками індустрії. Постачальник зобов'язаний розробляти такі плани з метою забезпечення дотримання конкретних показників часу відновлення, визначених у розділі 5.6 нижче.

5.6 Показники цільової точки відновлення («**RPO**») і цільового часу відновлення («**RTO**») для будь-якої Послуги, розміщеної на сервері, визначаються наступним чином: 24 години RPO та 24 години RTO; незважаючи на це, Постачальник забезпечуватиме відповідність будь-яким більш строгим показникам RPO або RTO, які Kyndryl зобов'язалася підтримувати для Замовника, негайно після отримання від Kyndryl письмового повідомлення про застосування коротших інтервалів RPO або RTO (повідомлення електронною поштою означає письмове повідомлення). Оскільки це стосується всіх інших Послуг, які Постачальник надає Kyndryl, Постачальник гарантуватиме, що його плани забезпечення безперервності бізнес-процесів і аварійного відновлення розроблені для дотримання значень RPO та RTO, забезпечуючи виконання зобов'язань Постачальника перед Kyndryl згідно з Документом Транзакції, відповідним базовим договором міжсторонами та цими Положеннями, включаючи зобов'язання щодо своєчасного тестування, підтримки та обслуговування.

5.7 Постачальник зобов'язаний здійснювати заходи, спрямовані на оцінювання, тестування та застосування рекомендованих виправлень безпеки до Послуг і Результатів, а також пов’язаних із ними систем, мереж, прикладних програм і базових компонентів у межах сфери дії таких Послуг і Результатів, а також систем, мереж, прикладних програм і базових компонентів, що використовуються для Взаємодії з Технологіями Kyndryl. Після визначення того, що рекомендоване виправлення є застосовним і відповідає вимогам, Постачальник повинен застосувати це виправлення відповідно до документально зафіксованих рекомендацій з урахуванням рівня важливості та ризиків. Реалізація рекомендованих виправлень захисту регламентується політикою Постачальника щодо керування змінами.

5.8 Якщо у Kyndryl є вагомі підстави вважати, що обладнання або програмне забезпечення, що надаються їй Постачальником, можуть містити елементи, які уможливлюють вторгнення, зокрема шпигунське програмне забезпечення, шкідливе програмне забезпечення або зловмисний код, Постачальник своєчасно співпрацюватиме з Kyndryl під час розслідування та виправлення моментів, що викликають занепокоєння Kyndryl.

6. Надання Послуг

6.1 Постачальник використовуватиме стандартні галузеві методи об'єднаної автентифікації для будь-яких користувачів Kyndryl або облікових записів Замовника, дотримуючись Кращих Практик індустрії автентифікації таких користувачів Kyndryl або облікових записів Замовника (таких як, наприклад, метод багатофакторного єдиного входу з централізованим керуванням з боку Kyndryl на основі OpenID Connect або Security Assertion Markup Language).

7. Субпідрядники. Без обмеження зобов'язань Постачальника або прав Kyndryl за Документом Транзакції або відповідним базовим договоромміж сторонами стосовно утримання субпідрядників Постачальник зобов'язаний подбати про те, аби кожен субпідрядник, який надає Постачальнику послуги, запровадив засоби управління та контролю для виконання вимог і зобов'язань, які встановлюються для Постачальника згідно з цими Положеннями.

8. Фізичні Носії. Постачальник зобов'язаний надійно виключити конфіденційну інформацію з фізичних носіїв, призначених для повторного використання, перед повторним використанням, а також знищити фізичні носії, не призначені для повторного використання, відповідно до Кращих Практик індустрії щодо очищення носіїв інформації.

Стаття IX. Сертифікати та звіти про Послуги, розміщені на сервері

Ця Стаття застосовується, якщо Постачальник надає Kyndryl Послуги, розміщені на сервері.

1.1 Постачальник повинен отримати такі сертифікати та звіти протягом зазначених нижче періодів часу:

Сертифікати / Звіти	**Період Часу**
Стосовно Послуг, розміщених на сервері, що надаються Постачальником: Сертифікат відповідності вимогам стандарту ISO 27001 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою», сертифікат видається на основі оцінки авторитетного незалежного аудитора **або** SOC 2 типу 2: звітавторитетного незалежного аудитора, який демонструє результати перевірки систем, засобів контролю та операцій Постачальника відповідно до SOC 2 типу 2 (включаючи, як мінімум, результати щодо захисту, конфіденційності та доступності).	Постачальник має отримати сертифікат відповідності вимогам ISO 27001 протягом 120 Днів від дати набуття чинності цього Документа Транзакції* або Дати Припущення** і далі має поновлювати сертифікат на основі оцінки авторитетного незалежного аудитора кожні 12 місяців після цього (відповідно до чинної на той момент версії стандарту) Постачальник повинен отримати звіт SOC 2 типу 2 протягом 240 днів від дати набуття цим Документом Транзакції* чинності або Дати Припущення** і далі повинен отримувати новий звіт від авторитетного незалежного аудитора, який демонструє результати перевірки систем, засобів контролю та операцій Постачальника відповідно до SOC 2 типу 2 (включаючи, як мінімум, результати щодо захисту, конфіденційності та доступності) кожні 12 місяців після цього. * Якщо з дати набуття чинності Постачальник надає Послугу, розміщену на сервері ** Дата, з якої Постачальник передбачає зобов'язання надавати Послугу, розміщену на сервері

1.2 Якщо Постачальник надасть письмовий запит, а Kyndryl письмово затвердить його, Постачальник може отримати сертифікат або звіт, еквівалентний по суті вищезазначеним сертифікатам або звітам, при цьому строки, зазначені в попередній таблиці, застосовуватимуться без змін для еквівалентного по суті сертифіката або звіту.

1.3 Постачальник зобов'язаний: (a) на запит своєчасно надати Kyndryl копію кожного сертифіката та звіту, який Постачальник повинен отримати; і (b) негайно усунути будь-які недоліки внутрішнього контролю, зазначені під час перевірок SOC 2 або по суті еквівалентних їм перевірок (за умови схвалення Kyndryl).

Стаття X. Співпраця, перевірка та виправлення

Ця Стаття застосовується, якщо Постачальник надає Kyndryl будь-які Послуги або Результати.

1. Співпраця з боку Постачальника

1.1 Якщо у Kyndryl є підстави сумніватися, що якісь Послуги або Результати могли сприяти, сприяють або сприятимуть будь-яким проблемам кібербезпеки, Постачальник зобов'язаний співпрацювати за будь-яким запитом Kyndryl щодо такої проблеми, у тому числі шляхом своєчасного та повного реагування на запити на отримання інформації шляхом надання документів, інших реєстраційних записів, проведення опитування відповідного Персоналу Постачальника тощо.

1.2 Сторони домовляються: (a) надавати на запит одна одній таку додаткову інформацію, (b) оформляти та передавати одна одній такі інші документи, і (c) здійснювати інші дії, яких може обґрунтовано вимагати інша сторона з метою реалізації наміру цих Положень і документів, зазначених у Положеннях. Наприклад, на запит Kyndryl Постачальник зобов'язаний вчасно надати умови щодо конфіденційності та безпеки, передбачені в письмових договорах із Суброзпорядниками та субпідрядниками, у тому числі шляхом надання доступу до самих договорів, якщо у Постачальника є таке право.

1.3 На запит Kyndryl Постачальник зобов'язаний вчасно надавати інформацію про те, в яких країнах були виготовлені, розроблені або іншим чином отримані його Результати та компоненти цих Результатів.

2. Перевірка (далі термін «Об'єкт» означає фізичну локацію, де Постачальник розміщує, обробляє або іншим чином отримує доступ до Матеріалів Kyndryl)

2.1 Постачальник зобов'язаний вести документацію, що демонструє відповідність цим Положенням, у форматі, що дозволяє провести перевірку (аудит).

2.2 Kyndryl, самостійно або разом із зовнішнім аудитором, може, письмово повідомивши Постачальника за 30 Днів, перевірити виконання Постачальником цих Положень, в тому числі шляхом доступу до будь-якого Об'єкта або Об'єктів для таких цілей, проте Kyndryl не матиме доступу до жодного центру обробки даних, в якому Постачальник обробляє Дані Kyndryl, якщо в неї не буде об'єктивних підстав вважати, що це необхідно для отримання потрібної інформації. Постачальник співпрацюватиме з Kyndryl під час проведення перевірки, у тому числі шляхом своєчасного та повного реагування на запити на отримання інформації шляхом надання документів, інших реєстраційних записів, проведення опитування відповідного Персоналу Постачальника тощо.Постачальник може надати підтвердження дотримання схваленого кодексу поведінки або галузевого механізму сертифікації або надати Kyndryl інформацію, яка може підтвердити виконання ним цих Положень.

2.3 Перевірка здійснюється не частіше одного разу протягом будь-якого 12-місячного періоду, крім випадків, коли: (a) Kyndryl перевіряє усунення Постачальником проблем, виявлених під час попередньої перевірки за 12-місячний період, або (b) сталося Порушення Безпеки і Kyndryl хоче перевірити, як виконуються зобов'язання, що стосуються порушення. У будь-якому разі Kyndryl надасть письмове повідомлення за 30 Днів, як зазначено в розділі 2.2 вище, але невідкладність усунення Порушення Безпеки може потребувати того, щоб Kyndryl провела перевірку з письмовим повідомленням менше ніж за 30 Днів.

2.4. Регуляторний орган або інший Володілець може користуватися тими самими правами, що й Kyndryl відповідно до розділів 2.2 та 2.3, при цьому регуляторний орган може користуватися додатковими правами, передбаченими законодавством.

2.5 Якщо Kyndryl має вагомі підстави вважати, що Постачальник не виконує будь-який пункт цих Положень (незалежно від того, чи виникли такі підстави внаслідок перевірки згідно з цими Положеннями чи іншим чином), Постачальник зобов'язаний негайно усунути таке невиконання.

3. Програма боротьби з контрафактною продукцією

3.1 Якщо Результати Постачальника включають електронні компоненти (наприклад, жорсткі диски, твердотільні накопичувачі, пам'ять, центральні процесори, логічні пристрої або кабелі), Постачальник зобов'язаний підтримувати та виконувати задокументовану програму запобігання підробкам, щоб у першу чергу — і найголовніше — запобігти наданню Постачальником контрафактних компонентів Kyndryl і, по-друге, негайно виявляти та виправляти всі випадки, коли Постачальник помилково надає Kyndryl контрафактні компоненти. Постачальник так само зобов'яже всіх своїх постачальників, які надають електронні компоненти, включені в Результати Постачальника для Kyndryl, використовувати та виконувати задокументовану програму запобігання підробкам.

4. Виправлення

4.1 Якщо Постачальник не виконує своїх зобов'язань за цими Положеннями і таке невиконання призводить до Порушення Безпеки, тоді Постачальник зобов'язаний усунути невиконання та виправити негативні наслідки Порушення Безпеки, виконавши відповідні дії згідно з обґрунтованими інструкціями та графіком Kyndryl. Якщо Порушення Безпеки виникає внаслідок надання Постачальником мультиарендної Послуги, розміщеної на сервері, і в подальшому впливає на велику кількість клієнтів Постачальника, включно з Kyndryl, тоді Постачальник зобов'язаний, з урахуванням характеру Порушення Безпеки, своєчасно і належним чином усунути невиконання та виправити негативні наслідки Порушення Безпеки, врахувавши належним чином будь-яку інформацію Kyndryl щодо таких виправлень. Без обмеження вищезазначеного Постачальник повинен без зайвого зволікання повідомити Kyndryl, якщо Постачальник більше не може виконувати зобов'язання, встановлені чинним законодавством про захист даних.

4.2 Kyndryl матиме право взяти участь у виправленні будь-якого Порушення Безпеки, описаного в розділі 4.1, як вона вважає за доцільне або необхідне, і Постачальник буде нести відповідальності за свої витрати на усунення невиконання, а також за витрати на виправлення та витрати, які несуть сторони, стосовно будь-якого такого Порушення Безпеки.

4.3 Наприклад, витрати на виправлення та витрати, пов'язані з Порушенням Безпеки, можуть включати витрати на виявлення та розслідування Порушення Безпеки, визначення обов'язків відповідно до чинного законодавства та нормативних актів, надання повідомлень про порушення, створення та забезпечення роботи кол-центрів, надання послуг моніторингу компенсацій і відновлення компенсацій, перезавантаження даних, виправлення дефектів продукту (включаючи за допомогою розробки Вихідного Коду чи іншої розробки), залучення сторонніх осіб для допомоги у виконанні попередніх або інших необхідних операцій, а також інші витрати, необхідні для виправлення/усунення негативних наслідків Порушення Безпеки. Для ясності: витрати на виправлення не включають втрати Kyndryl через упущену вигоду чи втрачених клієнтів, знецінення, шкоду для репутації або втрату очікуваних заощаджень.