第 1 条 連絡先個人情報

本条は、乙または Kyndryl が他方当事者の「BCI」を「処理」する場合に適用されます。

1.1 Kyndryl および乙は、乙による「サービス」および「成果物」のデリバリーに関連する業務を行う場合に他方当事者の「BCI」を「処理」することができます。

1.2 一方の当事者は、

a) 他のいかなる理由においても他方当事者の「BCI」を使用せず、または開示しないものとします (いずれの当事者も、事前に他方当事者の書面による同意を得ることなく、他方当事者の「BCI」を「販売」せず、またはマーケティングを目的として使用もしくは開示しないものとします。また、必要に応じて、影響を受ける「情報主体」の書面による同意を事前に得るものとします。)。さらに、

b) 他方当事者から書面で要求があり次第速やかに、他方当事者の「BCI」を削除し、修正し、訂正し、返却し、他方当事者の「BCI」の「処理」に関する情報を提供し、かかる「処理」を制限し、または他方当事者の「BCI」に関して合理的に要求されたその他の措置を講じるものとします。

1.3 両当事者は、各当事者の「BCI」に関する共同「管理者」関係を築くことを意味しておらず、また、「取引文書」のいずれの規定も、共同「管理者」関係の確立を企図することを表すとは解釈されないものとします。

1.4 https://www.kyndryl.com/privacy に記載の Kyndryl プライバシー・ステートメントに、Kyndryl による「BCI」の「処理」に関する追加の詳細情報があります。

1.5 両当事者は、他方当事者の「BCI」を喪失、破壊、改変、偶発的もしくは不正な開示、偶発的もしくは不正なアクセス、および違法な「処理」から保護するための技術的および組織的なセキュリティー対策を実施しており、今後も継続するものとします。

1.6 サプライヤーは、キンドリルの BCI に関連するセキュリティー・ブリーチを把握した場合、キンドリルに迅速に（いかなる場合も 48 時間以内に）通知するものとします。 サプライヤーはそのような通知を cyber.incidents@kyndryl.com に伝達します。乙は、当該侵害、ならびに乙の修復作業および復旧作業の状況に関して合理的に要求された情報を甲に提供します。例として、合理的に要求される情報には、「デバイス」、システムまたはアプリケーションに対する特権、管理者その他のアクセスを証するログ、「デバイス」、システムまたはアプリケーションの法的証拠となる画像、その他類似の項目を含むことがあります。ただし、これらは当該侵害または乙の修復および回復作業に関連する範囲に限ります。

1.7 乙が甲の「BCI」のみを「処理」しており、その他いかなる種類のデータもしくは資料、または甲の「会社システム」へのアクセス権限を有しない場合、本条および第 10 条 (協力、検証および修復) が、かかる「処理」に適用される唯一の条項となります。

第 2 条 技術的および組織的措置、データのセキュリティー

乙が甲の「BCI」以外の「Kyndryl データ」を「処理」する場合、本条が適用されます。乙は、すべての「サービス」および「成果物」を提供する際に、本条の要件に従うものとし、それにより、喪失、破壊、改変、偶発的もしくは不正な開示、偶発的もしくは不正なアクセス、および違法な形式の「処理」から「Kyndryl データ」を保護します。本条の要件は、乙が「成果物」および「サービス」の提供にあたって運用または管理するすべての IT アプリケーション、プラットフォームおよびインフラストラクチャー (すべての開発、テスト、ホスティング、サポート、運用およびデータ・センター環境を含みます。) に及びます。

1. データの利用

1.1. 乙は、甲の書面による同意を事前に得ることなく、「Kyndryl データ」に他の情報もしくはデータ (「個人情報」を含みます。) を追加し、またはこれらを「Kyndryl データ」に組み込まないものとします。また、乙は、「サービス」および「成果物」の提供を除くいかなる目的のために、集計された形式その他いかなる形式の「Kyndryl データ」も使用してはなりません (例として、乙は、新規オファリングの作成を意図した研究開発のために自らのオファリング改善の有効性もしくは手段を評価することを目的として、または自らのオファリングに関するレポートを生成することを目的として、「Kyndryl データ」を使用または再使用することは許可されていません。)。「取引文書」において明示的に許可されていない限り、乙は、「Kyndryl データ」の販売を禁止されています。

1.2. 乙は、「成果物」内に、または「サービス」の一環として、Web トラッキング・テクノロジー (HTML5、ローカル・ストレージ、第三者のタグまたはトークン、および Web ビーコンを含みます。) を組み込まないものとします。ただし、「取引文書」において明示的に許可されている場合は除きます。

2. 第三者の要請および機密保持

2.1. 乙は、甲より事前に書面で許可を得た場合を除き、いかなる第三者にも「Kyndryl データ」を開示しません。政府 (規制当局を含みます。) が「Kyndryl データ」へのアクセスを要求する場合 (例: 米国政府が「Kyndryl データ」取得のために乙に対する国家安全保障命令を送達した場合)、または「Kyndryl データ」の開示が法律により別途義務づけられている場合、乙は、かかる要求について甲に書面で通知し、かつ、開示に異議を申し立てる合理的な機会を甲に与えるものとします (法律により通知が禁止されている場合、乙は、裁判その他の手段を通じて「Kyndryl データ」の禁止または開示に異議を申し立てるために適切であると自らが合理的に判断する措置を取るものとします。)。

2.2. 乙は、(a)「サービス」または「成果物」を提供するために「Kyndryl データ」にアクセスする必要のある乙の従業員に、「サービス」および「成果物」を提供するために必要な範囲に限って、かかるアクセス権限が与えられること、および、(b) かかる従業員が、「本条件」で許可されている限りにおいて「Kyndryl データ」を使用し、開示することを要求された機密保持義務で拘束されていることを甲に保証します。

3. 「Kyndryl データ」の返却または削除

3.1. 乙は、甲の選択に従い、「取引文書」の解約後もしくは期間満了後、またはそれ以前の甲からの要求に応じて、「Kyndryl データ」を削除または返却します。甲が削除を要求した場合、乙は、「業界ベスト・プラクティス」に合致する方法で、当該データを判読不能にし、再アセンブルまたは再構成不可能にします。さらに、かかる削除について甲に証明するものとし

ます。甲が「Kyndryl データ」の返却を要求した場合、乙は、甲の合理的なスケジュールに従って、かつ、甲の書面による合理的な指示どおりに、返却を実行するものとします。

第3 条 プライバシー

乙が「Kyndryl 個人情報」を「処理」する場合、本条が適用されます。

1. 処理

1.1 甲は、甲の指示に従って「成果物」および「サービス」を提供することのみを目的として「Kyndryl 個人情報」を「処理」する「処理者」として乙を指名します。かかる指示には、「本条件」、両当事者間の「取引文書」および関連する基本契約に記載されているものが含まれます。乙がいずれかの指示に対応しなかった場合、甲は、書面で通知することにより、影響を受ける部分の「サービス」を解約することができます。指示がデータ保護法に違反していると乙が判断する場合、速やかに、かつ、法律により要求される期間内に、甲にその旨を通知します。

1.2 乙は、「サービス」および「成果物」に適用されるすべてのデータ保護法を遵守します。

1.3 「取引文書」の「補足」または「取引文書」自体において、「Kyndryl データ」に関して以下のことが定められています。

(a) 「情報主体」のカテゴリー。
(b) 「Kyndryl 個人情報」の種類。
(c) データ・アクションおよび「処理」対応。
(d) 「処理」の期間および頻度。
(e) 「復処理者」のリスト

2. 技術的および組織的措置

2.1 乙は、第 2 条 (「技術的および組織的措置、データのセキュリティー」) ならびに第 8 条 (「技術的および組織的措置、一般セキュリティー」) に定められた技術的および組織的措置を実装し、維持し、それにより、自らの「サービス」および「成果物」に存在するリスクに対する適切なセキュリティーレベルを確保します。乙は、第 2 条、本第 3 条および第 8 条における制限を認め、理解し、それらに従うものとします。

3. 情報主体の権利および要請

3.1 乙は、「情報主体」から届いた「Kyndryl 個人情報」に関する「情報主体」の権利行使の要求 (例: データの修正、削除およびブロッキング) について甲に速やかに (甲および「その他の管理者」が法律上の義務を履行することが可能なスケジュールで) 通知します。また、乙は、「情報主体」が Kyndryl に対してかかる要求を行うように速やかに指示することもできます。法律により義務づけられるか、または書面により甲から対応するよう指示される場合を除き、乙は「情報主体」からのいかなる要求にも応じないものとします。

3.2 「Kyndryl 個人情報」に関する情報を「その他の管理者」その他第三者 (例:「情報主体」または規制当局) に提供する義務が甲にある場合、乙は、かかる「その他の管理者」または第三者に対して甲が適時に対応可能なスケジュールで、甲の要求に応じてすべての情報を提供し、甲が要求する合理的なその他の措置を講じることによって速やかに甲を支援するものとします。

4. 復処理者

4.1 乙は、新規の「復処理者」の追加、または既存の「復処理者」による「処理」の適用範囲の拡大に先立ち、事前に書面で甲に通知するものとします。また乙は、かかる通知において、「復処理者」の名称を特定し、新規または拡大される「処理」の適用範囲を説明します。甲は、かかる新規の「復処理者」または拡大される適用範囲に対して合理的な根拠に基づいて随時異議を申し立てることができます。甲が異議を申し立てた場合、両当事者は、甲の異議申し立てに対処するために誠意をもって協力するものとします。甲が上記のとおり随時異議を申し立てる権利を条件として、甲が乙の書面通知から 30「日」以内に異議を提起しなかった場合、乙は、新規の「復処理者」に委託し、または既存の「復処理者」の適用範囲を拡大することができます。

4.2 乙は、「本条件」に定めるデータ保護、セキュリティーおよび認証に関する義務を、承認済みの各「復処理者」が「Kyndryl データ」の「処理」を開始する前に、「復処理者」に課すものとします。乙は、各「復処理者」による義務の履行について甲に全面的に責任を負います。

5. 域外でのデータ処理

以下で使用される用語は、次のとおりの意味を表します。

「十分国」とは、適用されるデータ保護法または規制当局の決定に基づき関連する転送について適切なレベルのデータ保護を提供する国をいいます。

「データ輸入者」とは、「十分国」で設立されたのではない「処理者」または「復処理者」をいいます。

「EU 標準契約条項」 (EU Standard Contractual Clauses 以下「EU SCC」といいます。) とは、第 9 条 (a) のオプション 1 および第 17 条のオプション 2 を除く選択条項が適用される「EU 標準契約条項」(委員会決定 2021/914) をいいます (以下で公式に公開されています。https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en)。

「セルビア標準契約条項」(Serbian Standard Contractual Clauses 以下「セルビア SCC」といいます。) とは、「Serbian Commissioner for Information of Public Importance and Personal Data Protection」(https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx に掲載) で採用されている「セルビア標準契約条項」をいいます。

「標準契約条項」(以下「**SCC**」といいます。) とは、「十分国」で設立されたのではない「処理者」への「個人情報」の転送について、適用されるデータ保護法により要求される契約条項をいいます。

EU 委員会標準契約条項の英国国際データ転送補遺（以下、「英国補足契約書」）とは、EU 委員会標準契約条項に対する英国の国際データ転送に関する補遺をいい、https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/で公式に公開されています。

EU 委員会標準契約条項のスイス補足契約書（以下、「スイス補足契約書」）とは、EU 委員会標準契約条項に付随し、スイスのデータ保護機関（以下、「**FDPIC**」）の決定に従い、かつスイスの連邦データ保護法（以下、「**FADP**」）に準拠して適用される契約条項を指します。

5.1　乙は、甲の書面による同意を事前に得ることなく、「Kyndryl 個人情報」を国境を超えて転送または開示しません (リモート・アクセスによる場合を含みます。)。甲がかかる同意を提供した場合、両当事者は、適用されるデータ保護法を確実に遵守するよう協力するものとします。かかる法律により「SCC」が義務づけられている場合、乙は、甲から要求があり次第速やかに「SCC」を締結します。

5.2　「EU SCC」に関して、

(a)　乙が「十分国」で設立されたのではない場合、乙は、「本条件」により、「データ輸入者」として甲と「EU SCC」を締結します。また、乙は、「EU SCC」第 9 条に従って、承認済みの各「復処理者」と書面契約を締結し、かかる合意のコピーを要求に応じて甲に提出します。

(i) 「EU SCC」の「モジュール 1」は、書面により別途両当事者が合意する場合を除き、適用されません。

(ii) 「EU SCC」の「モジュール 2」は、Kyndryl が「管理者」である場合に適用され、甲が「処理者」である場合は「モジュール 3」が適用されます。「EU SCC」の第 13 条に従い、「モジュール 2」または「モジュール 3」が適用される場合、両当事者は、(1) 「EU SCC」は、管轄権を有する監督機関が配置されている EU 加盟国の法律に準拠すること、(2) 「EU SCC」に起因するいかなる紛争も、管轄権を有する監督機関が配置されている EU 加盟国の裁判所で処理されることに合意します。(1) において、かかる法律が第三者の受益権を許容しない場合、「EU SCC」はオランダの法律に準拠するものとし、(2) における「EU SCC」に起因するいかなる紛争もオランダのアムステルダムの裁判所で解決されるものとします。

(b)　乙が「欧州経済地域」で設立され、Kyndryl が「一般データ保護規則 2016/679」の対象でない「管理者」である場合、「EU SCC」の「モジュール 4」が適用され、乙は「本条件」により、データ輸出者として甲と「EU SCC」を締結します。「EU SCC」の「モジュール 4」が適用される場合、両当事者は、「EU SCC」がオランダの法律に準拠するものとすること、および「EU SCC」に起因するいかなる紛争も、オランダのアムステルダムの裁判所で解決されるものとすることに合意します。

(c)　その他の「管理者」 (「お客様」または関連会社など) が第 7 条の「結合条約」に関連する「EU SCC」の当事者になることを要請する場合、乙は「本条件」により、かかるいかなる要請にも合意します。

(d)　「EU SCC」の「付録 II」を記入するのに必要な「技術的および組織的措置」が 「本条件」、両当事者間の「取引文書」自体および関連する基本契約に記載されています。

(e)　「EU SCC」と「本条件」の間に矛盾がある場合、「EU SCC」が優先します。

5.3 「英国補足契約書」について：

a) サプライヤー（乙）が十分性認定を受けた国（「十分国」）で設立されていない場合、(i) 乙は、甲（Kyndryl）を輸入者として「英国補足契約書」を締結し、本契約により、上記の EU SCC（処理活動の状況に応じて適用）を補足するものとし、かつ、(ii) 乙は、承認済みの各「復処理者」と書面による契約を締結し、要求に応じてこれらの契約のコピーを甲に提出するものとします。

b) 乙が「十分国」で設立され、甲が英国一般データ保護規則（2018 年 EU（離脱）法に基づき英国法に組み込まれたもの）の対象でない「管理者」である場合、乙は、輸出者として甲と「英国補足契約書」を締結し、本契約により、上記第 5 条 2 項 (b) に定める EU SCC を補足するものとします。

c) 顧客や関連会社などの「その他の管理者」が、「英国補足契約書」の当事者になることを要求した場合、乙は、本契約により、そうした要求すべてに同意するものとします。

d) 「英国補足契約書」の付録情報（表 3）は、該当する EU SCC、「本条項」、「取引文書」自体、および当事者間の関連する基本契約に記載されています。「英国補足契約書」が変更された場合、甲乙いずれの当事者も「英国補足契約書」を終了させることはできません。

e) 「英国補足契約書」と本規約の間に矛盾が生じた場合、「英国補足契約書」が優先されます。

5.4 「セルビア SCC」に関して、

(a) 乙が「十分国」で設立されたのではない場合、(i) 乙は、「本条件」により、乙自身を代表して「処理者」として甲と「セルビア SCC」を締結します。また、(ii) 乙は、「セルビア SCC」第 8 条に従って、承認済みの各「復処理者」と書面契約を締結し、かかる合意のコピーを要求に応じて甲に提出します。

(b) 乙が「十分国」で設立された場合、乙は、「本条件」により、「非十分国」を拠点とする各「復処理者」を代理して甲と「セルビア SCC」を締結します。乙がかかる「復処理者」のために「セルビア SCC」を締結できない場合、乙は、「復処理者」に「Kyndryl 個人情報」の「処理」を許可する前に、「復処理者」が署名済みの「セルビア SCC」を甲に提出し、甲が副署できるようにします。

(c) 甲と乙の間の「セルビア SCC」は、必要に応じて、「管理者」と「処理者」間の「セルビア SCC」、または「処理者」と「復処理者」間の書面による back-to-back 契約とみなすものとします。「セルビア SCC」と「本条件」の間に矛盾がある場合、「セルビア SCC」が優先します。

(d) 「非十分国」への「個人情報」の移転を管理するために「セルビア SCC」の「別紙 1」から「別紙 8」を記入するのに必要な情報は、「本条件」および「取引文書」の「別表」または「取引文書」自体に記載されている場合があります。

5.5 「スイス補足契約書」について：

(a) 第5.1項に基づくキンドリルの個人データ転送が スイスの連邦データ保護法（以下、「FADP」）の対象となる範囲においては、第5.2項で合意されたEU SCCが その転送に適用され、以下の修正によりスイスの個人データに関する一般データ保護規則（以下、「GDPR」）の標準を採用するものとします。

- 「GDPR」への言及は、FADPでそれに相当する条項への言及としても理解されるものとします。

- EU SCCの第13条および付録I.Cに基づき、スイス連邦データ保護情報コミッショナーは、管轄権を有する監督機関であるものとします。
- 転送がFADPのみに準拠する場合、スイスの法律が準拠法となります。
- EU SCC第18条の「加盟国」という語は、スイスのデータ主体がその常居所において権利を追求できるよう、スイスを含むように拡大されるものとします。

(b) なお、上記のいずれもが、EU SCCの提供するデータ保護のレベルを何らかの方法で低減することを意図したものではなく、当該の保護レベルをスイスのデータ主体に拡大することのみを目的としており、そうでない場合はEU SCC が優先されます。

6. 支援および記録

6.1 「処理」の性質を考慮して、乙は、「情報主体」の要求および権利に関連する義務を履行するための適切な技術的および組織的措置を設けることにより、甲を支援します。乙は、乙が入手可能な情報を考慮して、「処理」のセキュリティー、「セキュリティー侵害」の通知および連絡、ならびにデータ保護に関する影響評価の作成 (必要に応じて、責任を負う「規制当局」との事前協議を含みます。) に関する義務の遵守を確実にするために、甲を支援するものとします。

6.2 乙は、各「復処理者」(各「復処理者」の代表およびデータ保護担当者を含みます。) の名前および連絡先の詳細に関する最新の記録を維持します。要求に応じて、乙は、お客様その他第三者からの要求に対して甲が適時に対応可能なスケジュールで、この記録を甲に提出するものとします。

第 4 条 技術的および組織的措置、コードのセキュリティー

乙が「Kyndryl ソース・コード」へのアクセス権限を有する場合、本条が適用されます。乙は、本条の要件に従うものとし、それにより、喪失、破壊、改変、偶発的もしくは不正な開示、偶発的もしくは不正なアクセス、および違法な形式の「処理」から「Kyndryl ソース・コード」を保護します。本条の要件は、乙が「成果物」および「サービス」の提供、ならびに「Kyndryl テクノロジー」の「取り扱い」にあたって運用または管理するすべての IT アプリケーション、プラットフォームおよびインフラストラクチャー (すべての開発、テスト、ホスティング、サポート、運用およびデータ・センター環境を含みます。) に適用されます。

1. セキュリティー要件

以下で使用される用語は、次のとおりの意味を表します。

「禁止国」とは、次のいずれかをいいます。(a) 2019 年 5 月 15 日付け米国大統領令「情報通信技術およびサービスのサプライ・チェーンの保護 (Securing the Information and Communications Technology and Services Supply Chain)」の下で「外国の敵対者 (foreign adversary)」として指定されている国。(b) 2019 年米国国防権限法 (the U.S. National Defense Authorization Act of 2019) 第 1654 条に記載されている国。(c) 「取引文書」において「禁止国」として特定されている国。

1.1. 乙は、第三者の利益に資するエスクローに「Kyndryl ソース・コード」を配布せず、または置かないものとします。

1.2. 乙は、「禁止国」に配置されているサーバーに「Kyndryl ソース・コード」を置かないものとします。乙は、「禁止国」に所在している、または「禁止国」を訪問中のいかなる者 (自らの「担当者」を含みます。) にも (かかる訪問の範囲に限り)、理由および「Kyndryl ソース・コード」が配置されている国にかかわらず、「Kyndryl ソース・コード」へのアクセスまたは使用を許可しないものとします。また、乙は、かかるアクセスまたは使用を必要とする可能性がある開発、テストその他の作業を「禁止国」で行うことを許可しないものとします。

1.3. 乙は、法律または法解釈により「Kyndryl ソース・コード」を第三者に開示することが要求される法域に「Kyndryl ソース・コード」を置かず、または配布しないものとします。「Kyndryl ソース・コード」が配置されている法域において法律または法解釈が変更され、これにより当該「Kyndryl ソース・コード」を第三者に開示するよう乙に要求される可能性がある場合、乙は、当該「Kyndryl ソース・コード」を直ちに破棄し、またはかかる法域から直ちに撤去するものとします。また、かかる法律または法解釈が引き続き効力を有する場合、追加の「Kyndryl ソース・コード」をかかる法域に置かないものとします。

1.4. 乙は、乙、甲またはいずれかの第三者が 2019 年米国国防権限法の第 1654 条または第 1655 条に基づく開示義務を負う可能性がある措置 (契約の締結を含みます。) を直接的または間接的に取らないものとします。両当事者間の「取引文書」または関連する基本契約に明示的に許可されている場合を除き、乙は、いかなる状況の下でも、甲の書面による同意を事前に得ることなく、「Kyndryl ソース・コード」を第三者に開示することを許可されていません。

1.5. 甲が乙に対し、または第三者が一方当事者に対し、(a) 「禁止国」または上記第 1.3 条が適用される法域に乙が「Kyndryl ソース・コード」を持ち込めるようにしたこと、(b) 両当事者間の「取引文書」または関連する基本契約その他の契約で許可されていない方法で乙が「Kyndryl ソース・コード」を別途リリース、アクセスまたは使用したこと、(c) 乙が上記第 1.4 条に違反したことのいずれかを通知した場合、コモン・ロー、衡平法、または両当事者間の「取引文書」もしくは関連する基本契約その他の契約に基づく、かかる不遵守に対処する甲の権利を制限することなく、(i) かかる通知が乙宛ての場合、乙は、速やかに当該通知を

甲と共有し、(ii) 甲の合理的な裁量により、乙は、甲が (乙と協議後に) 合理的に決定するスケジュールで当該問題について調査し、改善するものとします。

1.6. サイバー・セキュリティー、知的財産の窃盗、または類似もしくは関連するリスク (かかる変更が行われない場合に甲の特定のお客様もしくは市場への販売が制限され、またはお客様のセキュリティーもしくはサプライ・チェーンの要件を満たすことができない可能性があるリスクを含みます。) に対処するために、「ソース・コード」のアクセスに関する乙のポリシー、手続き、管理または慣例を変更する必要があると甲が合理的に判断する場合、甲は、かかるリスクに対処するために必要な措置 (かかるポリシー、手続き、管理または慣例の変更を含みます。) について協議するために乙と連絡を取ることができます。甲から要求があり次第、乙は、かかる変更の必要性の評価および相互に合意した適切な変更内容の実施において甲に協力するものとします。

第 5 条 セキュアな開発

本条は、乙が自らもしくは第三者の「ソース・コード」もしくは「オンプレミス・ソフトウェア」を Kyndryl に提供する場合、または、乙のいずれかの「成果物」もしくは「サービス」が Kyndryl 製品もしくはサービスの一部として Kyndryl のお客様に提供される場合に適用されます。

1. セキュリティーの即応性

乙は、乙のいずれかの「成果物」に依存する甲の製品またはサービスのセキュリティーの即応性を評価する甲の社内プロセスに協力するものとします。これには、情報要求 (文書その他の記録、関連する乙の「担当者」との面談、またはこれらに類似するもの) に対し適時かつ十分に対応することが含まれます。

2. セキュアな開発

2.1 本第 2 条は、乙が Kyndryl に「オンプレミス・ソフトウェア」を提供している場合にのみ、適用されます。

2.2 「取引文書」の期間を通じて、乙は、「業界ベスト・プラクティス」に従い、(a) 乙または乙によって雇用される第三者が「成果物」用に、または「成果物」に関して、運用、管理、使用またはその他の方法で依拠するシステムおよび環境の開発、構築、テストおよび運用を保護するために、ならびに (b) すべての「成果物」のソース・コードを喪失、違法な形式の取り扱い、および不正なアクセス、開示または改変から保護するために必要なネットワーク、プラットフォーム、システム、アプリケーション、デバイス、物理的インフラストラクチャー、インシデント対応、ならびに「個人」に重点を置いたセキュリティー・ポリシー、手続き、および管理を実施しており、今後も継続するものとします。

3. ISO 20243認証

3.1 本第 3 条は、乙のいずれかの「成果物」または「サービス」が Kyndryl 製品またはサービスの一部として Kyndryl のお客様に提供される場合にのみ、適用されます。

3.2 乙は、国際標準化機構 (ISO) 20243 Information technology, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products (情報技術、オープンかつ信頼できるテクノロジー・プロバイダー、TM スタンダード (O-TTPS)、悪意を持って汚染された偽造製品の軽減) の遵守に関する認証 (自己評価、または信頼できる独立監査人の評価のいずれかに基づく認証) を取得するものとします。あるいは、乙が書面で要求し、甲が書面で承認した場合、乙は、セキュアな開発およびサプライ・チェーンの慣例に対処する、実質的に同等な業界標準の遵守に関する認証 (甲が承認した場合はその承認のとおり、自己評価、または信頼できる独立監査人の評価のいずれかに基づく認証) を取得するものとします。

3.3 乙は、国際標準化機構 (ISO) 20243 または (甲が書面で承認した場合) 実質的にこれに相当する業界標準の遵守に関する認証を、「取引文書」の発効日から 180「日」以内に取得し、その後 12 カ月ごとに当該認証を更新するものとします (該当する標準 (例: 国際標準化機構 (ISO) 20243、または甲が書面で承認した場合はセキュアな開発およびサプライ・チェーンの慣例に対処する実質的にこれに相当する業界標準) のその時点の現行バージョンに各認証を更新します。)。

3.4 乙は、上記の第 2.1 条および第 2.2 条に従って取得する義務がある認証のコピーを、要求があり次第、甲に提出するものとします。

4. セキュリティーの脆弱性

以下で使用される用語は、次のとおりの意味を表します。

「エラーの訂正」とは、「成果物」におけるエラーまたは欠陥 (「セキュリティーの脆弱性」を含みます。) を訂正するバグ修正および改訂をいいます。

「軽減策」とは、「セキュリティーの脆弱性」のリスクを軽減または回避する既知の手段をいいます。

「セキュリティーの脆弱性」とは、何者かによる攻撃を許す「成果物」の設計、コーディング、開発、実装、テスト、運用、サポート、メンテナンスまたは管理の状態のうち、不正なアクセスまたは利用につながるおそれがあるものをいい、これには次のいずれかが含まれます。(a) システムへのアクセス、システムの管理または運用妨害。(b) データへのアクセス、データの削除、改変または抽出。(c) ユーザーまたは管理者の ID、権限または許可の変更。「セキュリティーの脆弱性」は、共通脆弱性識別子 (Common Vulnerabilities and Exposures (CVE) ID)、または評価用の、もしくは正式な分類が割り当てられているかにかかわらず、存在することがあります。

4.1 乙は、自らが以下のすべてを行うことを表明し、保証します。(a)「セキュリティーの脆弱性」を特定するために「業界ベスト・プラクティス」を用いること。これには、静的および動的ソース・コード・アプリケーション・セキュリティー・スキャン、オープン・ソース・セキュリティー・スキャンおよびシステム脆弱性スキャンを通じて継続的に特定することが含まれます。(b)「成果物」における、ならびに乙が「サービス」および「成果物」の作成および提供にあたって使用するすべての IT アプリケーション、プラットフォームおよびインフラストラクチャーにおける「セキュリティーの脆弱性」の予防、検出、および訂正に役立てるために本条の要件を遵守すること。

4.2 乙が「成果物」またはかかる IT アプリケーション、プラットフォームもしくはインフラストラクチャーにおける「セキュリティーの脆弱性」を認識した場合、下表に定義された「重大度レベル」および期日に従って、すべてのバージョンおよびリリースの「成果物」についての「エラーの訂正」および「軽減策」を甲に提供するものとします。

重大度レベル (Severity Level)*
「セキュリティーの緊急的脆弱性」とは、「セキュリティーの脆弱性」のうち、重大かつ潜在的にグローバルな脅威となるものをいいます。甲は、CVSS 基本値 (Base Score) にかかわらず、自らの裁量により「セキュリティーの緊急的脆弱性」を決定します。
重大 – CVSS 基本値が 9 から 10.0 の「セキュリティーの脆弱性」
高 – CVSS 基本値が 7.0 から 8.9 の「セキュリティーの脆弱性」
中 – CVSS 基本値が 4.0 から 6.9 の「セキュリティーの脆弱性」
低 – CVSS 基本値が 0.0 から 3.9 の「セキュリティーの脆弱性」

期日				
緊急	***重大***	***高***	***中***	***低***
甲の機密保護最高責任者の判断に従い、4「日」以内。	30「日」	30「日」	90「日」	「業界ベスト・プラクティス」のとおり

*「セキュリティーの脆弱性」に即座に割り当てられる CVSS 基本値がない場合、乙は、かかる脆弱性の性質および状況に適切な重大度レベルを適用するものとします。

4.3 公開されている「セキュリティーの脆弱性」のうち、乙が「エラーの訂正」または「軽減策」を甲に提供していないものについて、乙は、脆弱性のリスクを軽減する可能性がある、技術的に実行可能な追加のセキュリティー管理を実装するものとします。

4.4 上記の「成果物」またはアプリケーション、プラットフォームもしくはインフラストラクチャーにおける「セキュリティーの脆弱性」に対する乙の対応に甲が満足しない場合、甲の他のいずれの権利にも不利益を与えることなく、乙は、乙の統括責任者、またはこれに相当する担当役員で「エラーの訂正」のデリバリーの責任者と甲が懸念事項について直接協議できるよう、甲のために速やかに調整するものとします。

4.5 「セキュリティーの脆弱性」の例として、第三者のコードまたはサポートを終了した (EOS) オープン・ソース・コードで、この種のコードがセキュリティー修正を受けていない場合が該当します。

第 6 条 会社システムのアクセス権限

乙の従業員が「会社システム」へのアクセス権限を有する場合、本条が適用されます。

1. 総則

1.1 甲は、乙の従業員に「会社システム」へのアクセス権限を与えるかを判断します。甲が権限を与える場合、乙は、本条の要件を遵守し、かかるアクセス権限を有する自らの従業員にもこれを遵守させるものとします。

1.2 甲は、乙の従業員が「会社システム」にアクセスすることができる手段を特定します。これには、当該従業員が甲の、または乙が提供する「デバイス」のいずれを介して「会社システム」にアクセスするかを含みます。

1.3 乙の従業員は、「サービス」提供のために、「会社システム」のみにアクセス可能であり、甲が当該アクセスを許可する「デバイス」のみを使用することができます。乙の従業員は、その他の者もしくは組織にサービスを提供するために、または「サービス」のための、もしくは「サービス」に関連する、乙もしくは第三者の IT システム、ネットワーク、アプリケーション、Web サイト、電子メール・ツール、コラボレーション・ツール、もしくは類似のものにアクセスするために、甲が当該アクセスを許可した「デバイス」を使用することはできません。

1.4 乙の従業員は、甲が「会社システム」へのアクセスを許可する「デバイス」を個人的な理由で使用できません (例: 乙の従業員は、音楽、動画、画像その他類似のアイテムなどのパーソナル・ファイルをかかる「デバイス」に保存してはならず、また、個人的な理由でかかる「デバイス」からインターネットを使用することはできません。)。

1.5 乙の従業員は、「会社システム」からアクセス可能な「Kyndryl 資料」を、甲の書面による事前承認を得ることなく、コピーしないものとします (さらに、いずれの「Kyndryl 資料」も、USB、外付けハード・ディスクその他類似のアイテムなどのポータブル・ストレージ・デバイスに決してコピーしないものとします。)。

1.6 要求に応じて、乙は、自らの従業員がアクセスを許可され、アクセスした特定の「会社システム」を、甲が特定する期間について従業員名によって確認するものとします。

1.7 乙は、「会社システム」にアクセス権限を有する自らの従業員が、(a) 乙による雇用が終了した場合、又は、(b) かかるアクセスを必要とする活動に従事しなくなった場合のいずれかに該当してから 24 時間以内に甲に通知するものとします。また、乙は、以前の、または現在の当該従業員のアクセス権限が直ちに確実に取り消されるよう甲と協業します。

1.8 乙は、実際のセキュリティー・インシデント (甲又は乙の「デバイス」の紛失、もしくは「デバイス」、データ、資料その他あらゆる種類の情報に対する不正なアクセスなど) 又はセキュリティー・インシデントの疑いがある場合、直ちに甲に報告し、かかるインシデントの調査において甲と協力するものとします。

1.9 乙は、甲の書面による同意を事前に得ることなく、いずれの代理人、独立契約者または従契約者にも、「会社システム」へのアクセスを許可してはなりません。甲がこの同意をした場合、乙は、これらの者が自らの従業員であるかのように、本条の要件を遵守するようこれらの者を契約で拘束するものとします。また、これらの者による当該「会社システム」へのアクセスに関するすべての作為または不作為について、乙が甲に対し責任を負うものとします。

2. デバイス・ソフトウェア

2.1 乙は、「会社システム」へのセキュアなアクセスを促進するために甲が要求するすべての「デバイス」ソフトウェアを適時にインストールするよう、自らの従業員に指示するものと

します。乙またはその従業員のいずれも、当該ソフトウェアの稼働、または当該ソフトウェアによって有効化されるセキュリティー機能の稼働を妨げないものとします。

2.2 乙およびその従業員は、甲が設定する「デバイス」構成ルールを遵守し、甲が意図するとおりのソフトウェア機能の確保に役立てるために甲と協業するものとします。例として、乙は、Web サイトブロック機能、または自動パッチ適用機能を無効にオーバーライドしないものとします。

2.3 乙は、「会社システム」にアクセスするために使用している「デバイス」、またはかかる「デバイス」のユーザー名、パスワードもしくは類似のものを、他者と共有してはなりません。

2.4 乙の「デバイス」を使用して「会社システム」にアクセスすることを甲が乙に許可した場合、乙は、甲が承認するオペレーティング・システムを当該「デバイス」にインストールして稼働させ、甲から指示を受けてから合理的な期間内に、かかるオペレーティング・システムの新規バージョンまたは新規のオペレーティング・システムにアップグレードするものとします。

3. 監督および協力

3.1 甲は、乙またはその従業員その他の者に事前に通知することなく、無条件に、甲が必要または適切であると判断するあらゆる方法、ロケーションおよび手段で潜在的な侵入その他のサイバー・セキュリティーの脅威をモニターし、修復することができます。例として、甲は、次のすべてを随時実行することができます。(a)「デバイス」にセキュリティー・テストを実施すること。(b)「デバイス」に保存されており、または「会社システム」経由で送信された通信 (任意の電子メール・アカウントからの電子メールを含みます。)、記録、ファイルその他のアイテムを、技術的その他の手段を通じてモニターし、復旧し、これらをレビューすること。(c) 「デバイス」の完全なフォレンジックイメージを取得すること。甲が自らの権利を行使するために乙の協力を必要とする場合、乙は、甲からのかかる協力要請 (例として、「デバイス」をセキュアに構成し、モニタリングその他のソフトウェアを「デバイス」にインストールし、システム・レベルの接続に関する詳細を共有し、「デバイス」に関するインシデント対応措置に着手し、甲が完全なフォレンジックイメージその他を取得するために甲に「デバイス」への物理的アクセスを提供するよう求めるもの、ならびにこれらに類似および関連するものが含まれます。) に完全かつ適時に応じるものとします。

3.2 甲は、自らを保護するために必要であると判断した場合、乙またはその従業員その他の者に事前に通知することなく、乙のいずれかの従業員または乙の全従業員の「会社システム」へのアクセス権限を随時取り消すことができます。

3.3 本条に定める甲の権利は、両当事者間の「取引文書」または関連する基本契約その他の契約のいずれの規定によっても、いかなる形でも妨害、低減または制限されません。かかる規定には、データ、資料その他あらゆる種類の情報を所定の場所にのみ保管することを要求できるもの、または所定の場所にいる者のみがかかるデータ、資料その他の情報にアクセスすることを要求できるものが含まれます。

4. Kyndryl デバイス

4.1 甲は、すべての「Kyndryl デバイス」に対する権限を維持し、当該「デバイス」の危険負担 (窃盗、器物破損または過失に対して支払うべき料金を含みます。) については乙が負うものとします。乙は、甲の書面による同意を事前に得ることなく、「Kyndryl デバイス」に対する改変を行わず、これを許可しないものとします。かかる改変とは「デバイス」に対する変

更を伴うものであり、これには「デバイス」ソフトウェア、アプリケーション、セキュリティー設計、セキュリティー構成、または物理的、機械的もしくは電子的設計の変更が含まれます。

4.2 乙は、「Kyndryl デバイス」が「サービス」を終了する必要が生じてから 5 営業日以内に、かかるすべての「デバイス」を返却します。また、甲が要求した場合は並行して、当該「デバイス」上のすべてのデータ、資料その他あらゆる種類の情報を永久に消去するために「業界ベスト・プラクティス」に従ってかかるすべてのデータ、資料その他の情報を破棄し、いかなるコピーも保持しないものとします。乙は、引き渡されたときと同じ状態で (通常の損耗は除きます。) 自らの費用負担で「Kyndryl デバイス」を梱包し、甲が特定するロケーション宛てに返却します。乙が本第 4.2 条におけるいずれかの義務を遵守しなかった場合、「取引文書」および関連する基本契約ならびに関連するいかなる甲乙間の契約の重大な違反となります。契約書に基づき乙が「会社システム」にアクセスすることで乙の作業その他の活動が促進される場合、かかる契約書も「関連する」契約と理解されます。

4.3 甲は、「Kyndryl デバイス」のサポート (「デバイス」の検査ならびに予防的メンテナンスおよび修復メンテナンスを含みます。) を提供します。乙は、修復サービスが必要な際に甲に速やかに通知するものとします。

4.4 甲が所有し、または使用を許諾する権利を有するソフトウェア・プログラムについて、甲は、乙が許可されている「Kyndryl デバイス」の使用をサポートするために使用し、保存し、十分なコピーを作成する一時的な権利を乙に付与します。法律の強行規定がある場合を除き、乙は、プログラムの他者への転送、ソフトウェア・ライセンス情報のコピー作成、またはプログラムの逆アセンブル、逆コンパイル、リバース・エンジニアリング、その他翻案を行うことはできません。

5. 更新

5.1 両当事者間の「取引文書」または関連する基本契約において、これに矛盾する定めがあろうとも、乙に書面で通知したうえで、かつ、乙の同意を得る必要なく、甲は、適用法の下の要件もしくはお客様の義務に対処するため、セキュリティーのベスト・プラクティスを開発に反映させるため、または「会社システム」もしくは自らの保護に必要であると甲が判断するその他の目的で、本条を更新し、補足し、その他修正することができます。

第 7 条 役務提供委託

本条は、乙の従業員が「サービス」を甲に提供するために自らのすべての作業時間を費やし、甲もしくはお客様の施設において、または乙の従業員の自宅からこれらすべての「サービス」を提供し、かつ、「会社システム」にアクセスするために「Kyndryl デバイス」を使用して「サービス」の提供のみを行う場合に適用されます。

1. 「会社システム」へのアクセス、甲の環境

1.1 乙は、甲が提供する「デバイス」を使用して「会社システム」にアクセスすることで、「サービス」の提供のみを行うことができます。

1.2 乙は、「会社システム」へのすべてのアクセスについて、第 6 条 (「会社システム」のアクセス権限) に定める条件を遵守するものとします。

1.3 甲から提供される「デバイス」は、乙およびその従業員が「サービス」の提供に使用することができる唯一の「デバイス」であり、乙およびその従業員のみが「サービス」の提供に使用することができます。いかなる場合も、乙またはその従業員は、「サービス」提供のために他の「デバイス」を使用してはならず、また、乙の他の顧客のために、または甲への「サービス」提供以外の目的で「Kyndryl デバイス」を使用できません。

1.4 「Kyndryl デバイス」を使用している乙の従業員は、「Kyndryl 資料」を相互に共有し、かかる資料を「Kyndryl デバイス」に保存することができます。ただし、かかる共有および保存は、「サービス」を完全に提供するために必要な範囲に限ります。

1.5 「Kyndryl デバイス」内へのかかる保存に関するものを除き、いかなる場合も、乙またはその従業員は、甲が保持している甲のリポジトリー、環境、ツールまたはインフラストラクチャーから「Kyndryl 資料」を除去してはならないものとします。

1.6 乙およびその従業員は、甲の書面による同意を事前に得ることなく、乙のリポジトリー、環境、ツールまたはインフラストラクチャー、その他乙のシステム、プラットフォーム、ネットワークまたは類似のものに「Kyndryl 資料」を転送することを許可されていません。

1.7 乙の従業員が「サービス」を甲に提供するために自らのすべての作業時間を費やし、甲もしくはお客様の施設において、または乙の従業員の自宅からこれらすべての「サービス」を提供し、かつ、「会社システム」にアクセスするために「Kyndryl デバイス」を使用して「サービス」の提供のみを行う場合、第 8 条 (「技術的および組織的措置、一般セキュリティー」) は乙の「サービス」に適用されません。その他の場合、第 8 条は乙の「サービス」に適用されます。

第 8 条 技術的および組織的措置、一般セキュリティー

乙が甲に「サービス」または「成果物」を提供する場合 (ただし、かかる「サービス」または「成果物」の提供において甲の「BCI」のみにアクセス権限を有する場合は除きます。例: 乙がその他「Kyndryl データ」を「処理」せず、または他の「Kyndryl 資料」もしくは「会社システム」へのアクセス権限を有しないなど)、乙の「サービス」および「成果物」のみが Kyndryl に「オンプレミス・ソフトウェア」を提供している場合、または乙が第 7 条 (その第 1.7 条を含みます。) に従って役務提供委託モデルで自らのすべての「サービス」または「成果物」を提供する場合、本条が適用されます。

乙は、本条の要件に従うものとし、それにより、(a) 喪失、破壊、改変、偶発的もしくは不正な開示、偶発的もしくは不正なアクセスから「Kyndryl 資料」を、(b) 違法な形式の「処理」から「Kyndryl データ」を、(c) 違法な形式の「取り扱い」から「Kyndryl テクノロジー」を保護します。本条の要件は、乙が「成果物」および「サービス」の提供、ならびに「Kyndryl テクノロジー」の「取り扱い」にあたって運用または管理するすべての IT アプリケーション、プラットフォームおよびインフラストラクチャー (すべての開発、テスト、ホスティング、サポート、運用およびデータ・センター環境を含みます。) に適用されます。

1. セキュリティー・ポリシー

1.1. 乙は、乙のビジネスに不可欠であり、乙の全従業員に義務づけられ、かつ、「業界ベスト・プラクティス」に合致する IT セキュリティー・ポリシーおよび慣例を維持し、これに従います。

1.2. 乙は、自社の IT セキュリティー・ポリシーおよび慣例を少なくとも年に一度見直し、「Kyndryl 資料」を保護するために乙が必要と判断する場合、それらを修正します。

1.3. 乙は、新規採用者全員について、標準の必須な雇用確認要件を維持し、これに従います。また、当該要件の遵守を乙の「担当者」および「乙の関連会社」においても実施します。これらの要件には、犯罪歴の調査 (適用法令によって調査が可能な場合に限る)、身元証明の確認、および乙が必要であるとみなす追加のチェックを含みます。ただし、日本国内で行われる取引においては犯罪歴の調査は含まれないものとします。乙は、自身が必要であるとみなす場合に応じて、これらの要件を定期的に繰り返し再確認します。

1.4. 乙は、年に一度、自社の従業員にセキュリティーおよびプライバシーの教育を行い、かかるすべての従業員に対し、乙の行動規範または類似する文書に規定されるとおり、各自が乙の倫理的な行動基準、機密保持義務およびセキュリティー・ポリシーの遵守について毎年宣誓することを求めるものとします。乙は、「サービス」、「成果物」または「Kyndryl 資料」のコンポーネントに対する管理者としてのアクセスが認められた者に対して、要求される遵守および認定を維持するための必要性に応じて、「サービス」、「成果物」および「Kyndryl 資料」に関するそれぞれの役割とサポートに特化されたトレーニングと共に、ポリシーおよび手順に関する追加的なトレーニングを実施します。

1.5. 乙は、すべての「サービス」および「成果物」ならびに「Kyndryl テクノロジー」のすべての「取り扱い」において、「Kyndryl 資料」を保護し、その可用性を維持するために、セキュリティーおよびプライバシー措置を設計するものとします (セキュリティー・バイ・デザインおよびプライバシー・バイ・デザイン、セキュアなエンジニアリングおよび運用を要求するポリシーおよび手順による実施、保守および遵守によることを含みます。)。

2. セキュリティー・インシデント

2.1. 乙は、コンピューターのセキュリティー・インシデントの取り扱いについての「業界ベスト・プラクティス」ガイドラインに合致する、文書化されたインシデント対応ポリシーを維持管理し、これに従います。

2.2. 乙は、「Kyndryl 資料」の不正なアクセスまたは使用を調査し、適切な対応計画を定め、実行します。

2.3. サプライヤーはセキュリティー・ブリーチを把握した場合、キンドリルに迅速に（いかなる場合も 48 時間以内に）通知するものとします。 サプライヤーはそのような通知を cyber.incidents@kyndryl.com に伝達します。乙は、当該侵害、ならびに乙の修復作業および復旧作業の状況に関して合理的に要求された情報を甲に提供します。例として、合理的に要求される情報には、「デバイス」、システムまたはアプリケーションに対する特権、管理者その他のアクセスを証するログ、「デバイス」、システムまたはアプリケーションの法的証拠となる画像、その他類似の項目を含むことがあります。ただし、これらは当該侵害または乙の修復および回復作業に関連する範囲に限ります。

2.4. 乙は、「セキュリティー侵害」に関する甲、甲の関連会社およびお客様 (ならびにこれらの顧客および関連会社) の一切の法律上の義務 (規制当局または「情報主体」に通知する義務を含みます。) を履行するために合理的な支援を甲に提供するものとします。

2.5. 乙は、甲が書面により承認する場合、または法律により義務づけられている場合を除き、「セキュリティー侵害」が直接的または間接的に Kyndryl または「Kyndryl 資料」に関連することを第三者に報告または通知しないものとします。法律上必要な通知が Kyndryl の識別情報を直接的または間接的に公開する場合、乙は、第三者に当該通知を送付する前に書面により甲に通知するものとします。

2.6. 乙が「本条件」に基づくいずれかの義務に違反したことにより「セキュリティー侵害」が生じた場合、以下の項目が適用されます。

(a) 乙は、該当する規制当局、その他の政府機関および関連する業界の自主規制機関、メディア (適用法により義務づけられている場合)、「情報主体」、お客様その他の者に対して「セキュリティー侵害」の通知を行う際に、自らに発生する費用および甲に発生する実費について負担するものとします。

(b) 甲が要求した場合、乙は自ら費用を負担して、「情報主体」からの「セキュリティー侵害」に関する質問に回答するためにコール・センターを設立し、その後、当該「情報主体」が「セキュリティー侵害」の通知を受けた日付から 1 年間、またはデータ保護法で義務づけられている期間のうち、より手厚い保護が与えられる期間、維持するものとします。甲および乙は、問い合わせ対応時にコール・センターのスタッフが使用する原稿その他の資料を作成するために協力するものとします。乙にコール・センターを設立させる代わりに、甲は乙に対し書面で通知することにより、自己のコール・センターを設立し、維持することができます。その場合、乙は、当該コール・センターの設立および維持に際し甲に発生する実費を負担するものとします。

(c) 乙は、当該侵害による影響を受け、当該サービスに登録することを選択した個人が「セキュリティー侵害」の通知を受けた日付から 1 年間、またはデータ保護法で義務づけられている期間のうち、より手厚い保護が与えられる期間、クレジット・モニタリングおよびクレジット・リストア・サービスの提供に際し甲に発生する実費を負担するものとします。

3. 物理的セキュリティーおよび入場管理 (以下で使用される「設備」とは、乙が「Kyndryl 資料」をホストし、処理し、またはこれにアクセスする物理的ロケーションをいいます。)

3.1. 乙は、「設備」への不正な入場から保護するため、適切に物理的な入場管理 (柵、カード制御の入口、監視カメラ、および有人の受付デスクなど) を維持管理します。

3.2. 乙は、「設備」および「設備」内の管理区域へのアクセス (一時的なアクセスを含みます。) に権限ある承認を要求し、職務内容および業務上の必要性によってアクセスを制限します。乙が一時的なアクセスを認める場合、「設備」および管理区域内では権限のある従業員が訪問者に同行します。

3.3. 乙は、「設備」内の管理区域に入場することを適切に制限するために物理的アクセス制御 (「業界ベスト・プラクティス」に合致する多要素アクセス制御を含みます。) を導入し、すべての入場の試みを記録し、当該ログを少なくとも 1 年間保持します。

3.4. 乙は、(a) アクセス権限を有する乙の従業員の離職時に、または (b) 当該従業員がアクセスについて有効な業務上の必要性がなくなった時点で、「設備」および管理区域へのアクセス権限を取り消します。乙は、文書化された正式な離職手続き (アクセス制御リストからの速やかな削除、物理的なアクセス・バッジの返却などを含みます。) に従います。

3.5. 乙は、「サービス」および「成果物」ならびに「Kyndryl テクノロジー」の「取り扱い」をサポートするために使用されるすべての物理的インフラストラクチャーを自然発生的および人為的な環境脅威 (極端な周辺温度、火災、洪水、湿度、窃盗、および破壊行為など) から保護するための予防措置を講じます。

4. アクセス、介入、転送、および分離の管理

4.1. 乙は、「サービス」の運用、「成果物」の提供、および「Kyndryl テクノロジー」の「取り扱い」において乙が管理する文書化されたネットワークのセキュリティー・アーキテクチャーを維持します。乙は、安全な分割、分離および防御の詳細な基準を遵守するために、かかるネットワーク・アーキテクチャーを個別にレビューし、システム、アプリケーションおよびネットワーク装置に対する不正なネットワーク接続を防止するための措置を講じます。乙は、「ホスト・サービス」のホスティングおよび運用において無線技術を使用することはできません。その他の場合、乙は、「サービス」および「成果物」のデリバリー、ならびに「Kyndryl テクノロジー」の「取り扱い」において、無線ネットワーク技術を使用することができます。ただし、乙は、当該無線ネットワークにおいて暗号化し、セキュア認証を要求するものとします。

4.2. 乙は、「Kyndryl 資料」がアクセス権限のない個人に公開され、または権限のない個人のアクセスを許す状態から論理的に分離し、それらの事象を防止する措置を維持します。さらに、乙は、実稼動、非実稼動およびその他の環境の適切な分離を維持し、「Kyndryl 資料」が非実稼動環境に転送される場合 (例えば、エラーの複製など) は、乙は非実稼動環境のセキュリティーおよびプライバシー保護が実稼動環境と等しいことを保証します。

4.3. 乙は、転送時および保管時に「Kyndryl 資料」を暗号化します (保管時の「Kyndryl 資料」の暗号化が技術的に実行不可能であることを、甲が合理的に納得できるように乙が示す場合を除きます。)。乙はまた、該当する場合、すべての物理的メディア (バックアップ・ファイルを含むメディアなど) を暗号化します。乙は、データの暗号化に関連するセキュリティー保護されたキーの生成、発行、配布、保管、ローテーション、失効、リカバリー、バックアップ、破棄、アクセス、および使用に関する手続きを文書化し、維持管理します。乙は、当該暗号化のために使用される特定の暗号化方式が「業界ベスト・プラクティス」(例: NIST SP 800-131a) に一致していることを保証するものとします。

4.4. 乙が「Kyndryl 資料」へのアクセスを必要とする場合、乙は、当該アクセスを「サービス」および「成果物」の提供およびサポートに必要な最小限のレベルに制限します。乙については、基盤となるコンポーネントに対する管理者としてのアクセス権 (特権アクセス権) を含む当該アクセス権は、個人・役割に基づくもので、職務分離の原則に従って、権限のある乙の従業員による承認および定期的な確認が行われることが必要です。乙は、重複アカウントおよび休止アカウントを特定し、削除するための措置を維持管理します。また、乙は、アカウント所有者の離職後、または甲、もしくは権限のある乙の従業員 (アカウント所有者のマネージャーなど) の要求から 24 時間以内に、特権アクセス権の付帯するアカウントを取り消すものとします。

4.5. 「業界ベスト・プラクティス」に従って、乙は、非アクティブ・セッションのタイムアウト、複数回連続でログインを試みて失敗したアカウントのロックアウト、強力なパスワードまたはパスフレーズによる認証を強制する技術的手段、ならびに当該パスワードおよびパスフレーズの安全な転送および保管を要求する手段を維持します。乙は、「Kyndryl 資料」に対するすべての非コンソール・ベースの特権的アクセスにおいて多要素認証を使用します。

4.6. 乙は、特権アクセス権の使用をモニターし、以下を目的として策定された、セキュリティー情報およびイベント管理の措置を維持します。(a) 不正アクセスおよび不正なアクティビティーの特定、(b) 当該アクセスおよびアクティビティーに対するタイムリーかつ適切な対応の促進、ならびに (c) 文書化された乙のポリシーへの準拠に関する、乙、甲 (「本条件」における検証する権利、ならびに両当事者間の「取引文書」または関連する基本契約その他の関連する契約における監査権に基づく)、その他による監査の実施。

4.7. 乙は、「業界ベスト・プラクティス」に従って、「サービス」または「成果物」の提供および「Kyndryl テクノロジー」の「取り扱い」にあたって使用するシステムに対する、またはかかるシステムに関する、すべての管理者、ユーザーその他のアクセス権限またはアクティビティーを記録したログを保持します (また、要求に応じてそれらのログを甲に提供します。)。乙は、当該ログについて、不正アクセス、変更、および偶発的または故意による破壊から保護する対策を維持します。

4.8. 乙は、当該保護により、自らが所有または管理するシステム (エンドユーザー・システムを含みます。)、ならびに「サービス」もしくは「成果物」の提供または「Kyndryl テクノロジー」の「取り扱い」にあたって使用システムのコンピューティング保護を維持します。この保護には、エンドポイント・ファイアウォール、フルディスク暗号化、マルウェアおよび APT 攻撃に対処するためのシグニチャー・ベースおよび非シグニチャー・ベースのエンドポイント検出および対応技術、タイム・ベースの画面ロック、ならびにセキュリティー構成およびパッチ適用要件を強制するエンドポイント管理ソリューションなどが含まれます。乙は、既知の、かつ信頼されたエンドユーザー・システムのみに乙のネットワークの使用が許可されるようにする、技術的な運用管理を行います。

4.9. 「業界ベスト・プラクティス」に従って、乙は、「Kyndryl 資料」が存在し、または処理されるデータ・センター環境の保護を維持します。この保護には侵入の検出および防止ならびにサービス妨害攻撃の対策および軽減が含まれます。

5. サービスおよびシステムの完全性および可用性管理

5.1. 乙は、以下のことを行います。(a) セキュリティーおよびプライバシー・リスク・アセスメントを少なくとも年に一度実施する。(b) 「サービス」および「成果物」に関しては実稼動リリースの前およびその後年に一度、「Kyndryl テクノロジー」の「取り扱い」に関しては年に一度、セキュリティー・テストおよび脆弱性アセスメントを実施する (自動化されたシステムおよびアプリケーションのセキュリティー・スキャン、ならびに手動の倫理的ハッキングを含みます。)。(c) 適格な独立した第三者に、「業界ベスト・プラクティス」に合致する侵入テスト (自動化されたテストおよび手動のテストを含みます。) を少なくとも年に一度実施することを依頼する。(d) 「サービス」および「成果物」の各コンポーネントについての、ならびに「Kyndryl テクノロジー」の「取り扱い」に関するセキュリティー構成要件の遵守について、自動化された管理およびルーチン検証を実施する。(e) 関連するリスク、悪用の可能性、および影響に基づいて、特定された脆弱性またはセキュリティー構成要件の不遵守を修復する。乙は、修復作業のテスト、評価、スキャンおよび実行を実施する際は、「サービス」の中断を回避するよう合理的な手段を講じます。甲の要求に応じて、乙は、乙のその時点で最新の侵入テスト・アクティビティーの書面による概要を甲に提供します。報告書には、少なくとも、テストの対象となるオファリングの名称、テストの範囲に含まれるシステムまたはアプリケーションの数、テストの日付、テストに使用した方法ならびに所見の大まかな概要を含むものとします。

5.2. 乙は、「サービス」もしくは「成果物」の変更、または「Kyndryl テクノロジー」の「取り扱い」に対する変更の適用に関連するリスクの管理を目的として設計されたポリシーおよび手続きを維持します。かかる変更 (影響を受けるシステム、ネットワークおよび基礎となるコンポーネントに対するものを含みます。) を実行する前に、乙は、変更要請に次のものをすべて文書化します。(a) 変更事項およびその理由、(b) 実施詳細およびスケジュール、(c)

「サービス」および「成果物」、「サービス」の顧客、または「Kyndryl 資料」に対する影響に対処するリスク・ステートメント、(d) 予期される結果、(e) ロールバック計画、(f) 権限のある乙の従業員による承認。

5.3. 乙は、「サービス」の運用、「成果物」の提供、および「Kyndryl テクノロジー」の「取り扱い」にあたって使用するすべての IT 資産のインベントリーを維持管理します。乙は、当該 IT 資産、「サービス」、「成果物」および「Kyndryl テクノロジー」(これらの基礎となるコンポーネントを含みます。) の正常性 (機能を含みます。) および可用性を継続的に監視し、管理します。

5.4. 乙は、あらかじめ提供されるシステム・セキュリティー・イメージまたはセキュリティー基準に基づいて、「サービス」および「成果物」の開発または運用、ならびに「Kyndryl テクノロジー」の「取り扱い」にあたって使用するすべてのシステムを構築し、それらは、Center for Internet Security (CIS) のベンチマークなどの「業界ベスト・プラクティス」を満たすものとします。

5.5. 両当事者間の「取引文書」または関連する基本契約に基づく、事業継続に関する乙の義務または甲の権利を制限することなく、乙は、事業および IT の継続性ならびに災害復旧要件について、各「サービス」および「成果物」、ならびに「Kyndryl テクノロジー」の「取り扱い」にあたって使用する各 IT システムを、文書化されたリスク管理ガイドラインに従って個別に評価します。乙は、かかる各「サービス」および「成果物」ならびに IT システムについて、当該リスク・アセスメントで保証される範囲において、「業界ベスト・プラクティス」に合致する事業および IT 継続性および災害復旧の計画が個別に定義、文書化、維持され、年に一度検証されることを保証するものとします。乙は、下記第 5.6 条に定める特定のリカバリー時間を提供するよう当該計画が設計されていることを保証するものとします。

5.6. 「ホスト・サービス」に関する特定のリカバリー・ポイント目標 (以下「**RPO**」といいます。) およびリカバリー時間の達成目標 (以下「**RTO**」といいます。) は、それぞれ 24 時間です。ただし、より短時間の「RPO」または「RTO」を甲がお客様に約束した場合、乙は、かかる「RPO」または「RTO」について甲から書面で通知を受けてから速やかに、より短時間の「RPO」または「RTO」を遵守するものとします (電子メールは書面とみなします。)。乙から甲に提供されるその他すべての「サービス」に関して、乙は、自らの事業継続および災害復旧の計画が、両当事者間の「取引文書」および関連する基本契約、ならびに「本条件」に基づく、甲に対する乙のすべての義務 (テスト、サポートおよびメンテナンスを適時に提供する義務を含みます。) を引き続き遵守することが可能となる「RPO」および「RTO」を提供するよう設計されていることを保証するものとします。

5.7. 乙は、「サービス」および「成果物」、ならびに「サービス」および「成果物」の範囲内の関連するシステム、ネットワーク、アプリケーションおよび基盤となるコンポーネント、ならびに「Kyndryl テクノロジー」の「取り扱い」に使用するシステム、ネットワーク、アプリケーションおよび基盤となるコンポーネントを評価し、テストし、それらにセキュリティー・アドバイザリー・パッチを適用することを目的として設計された措置を維持します。セキュリティー・アドバイザリー・パッチが適用可能かつ適切であると判断されれば、乙は、文書化された重大度およびリスクに関するアセスメント・ガイドラインに従って当該パッチを実装します。乙によるセキュリティー・アドバイザリー・パッチの実装には、乙の変更管理ポリシーが適用されます。

5.8. 乙が甲に提供するハードウェアまたはソフトウェアに侵入の要素 (スパイウェア、マルウェアまたは悪意あるコードなど) が含まれている可能性があると甲が判断する合理的な根拠がある場合、乙は、甲の懸念事項を調査および修復するにあたって甲に適時に協力するものとします。

6. サービスの提供

6.1 乙は、甲のユーザーまたはお客様のアカウントのために業界で一般的な方法であるフェデレーション認証をサポートし、かかる甲のユーザーまたはお客様のアカウントの認証において「業界ベスト・プラクティス」に従うものとします (甲が集中管理する多要素シングル・サインオンにより、OpenID Connect または Security Assertion Markup Language を使用するなど)。

7. **「復処理者」** 両当事者間の「取引文書」または関連する基本契約に基づく、従契約者の維持に関する乙の義務または甲の権利を制限することなく、乙は、自らのために作業を履行する従契約者が、「本条件」より乙に課される要件および義務を遵守するためのガバナンス・コントロールを設けていることを保証するものとします。

8. **物理メディア** 乙は、メディアのサニタイズに関する「業界ベスト・プラクティス」に従って、再利用を意図する物理メディアを再利用する前にサニタイズを安全に行い、かつ再利用を意図しない物理メディアを破棄するものとします。

第 9 条 ホスト・サービスの認証および報告書

乙が甲に「ホスト・サービス」を提供する場合、本条が適用されます。

1.1 乙は、下記に定める期日内に、以下の認証または報告書を取得するものとします。

認証 / 報告書	**期日**
乙のホスト・サービスに関して 国際標準化機構 (ISO) 27001、情報技術、セキュリティー技術、情報セキュリティー・マネジメントシステムの遵守に関する認証。かかる認証は、信頼できる独立監査人に基づくものとします。 **または** SOC 2 Type 2: 信頼できる独立監査人による、乙のシステム、制御および運用のレビュー (少なくともセキュリティー、機密性および可用性を含みます。) を証する、SOC 2 Type 2 に従った報告書	乙は、国際標準化機構 (ISO) 27001 認証を、「取引文書」の発効日*または引受け日**から 120「日」以内に取得し、その後信頼できる独立監査人の評価に基づいて 12 カ月ごとに当該認証を更新するものとします (その時点の現行バージョンに各認証を更新します。)。 乙は、「取引文書」の発効日*または引受け日**から 240「日」以内に SOC 2 Type 2 報告書を取得し、その後信頼できる独立監査人による、乙のシステム、制御および運用のレビュー (少なくともセキュリティー、機密性および可用性を含みます。) を証する、SOC 2 Type 2 に従った新規報告書を 12 カ月ごとに取得するものとします。 * 当該発効日の時点で乙が「ホスト・サービス」を提供している場合。 ** 乙の「ホスト・サービス」を提供する義務が発生する日付。

1.2 乙が書面で要求し、甲が書面で承認した場合、乙は、実質的に上記のものに相当する認証または報告書を取得することができます。その際、実質的に相当する認証または報告書に関して、上記の表に定められた期日が変更されずに適用されると理解します。

1.3 乙は、(a) 要求があり次第、取得する義務がある各認証および報告書のコピーを速やかに甲に提出し、(b) SOC 2 または実質的にこれに相当するもの (甲が承認した場合) のレビューにおいて挙げられた社内制御の弱点を速やかに解決するものとします。

第 10 条 協力、検証および修復

乙が甲に「サービス」または「成果物」を提供する場合、本条が適用されます。

1. 乙の協力

1.1. 「サービス」または「成果物」がサイバー・セキュリティーの懸念事項に寄与したか、寄与しているか、または寄与するかについて、甲が疑問を抱く場合は、乙は、かかる懸念事項に関する甲からの問い合わせに合理的に協力するものとします。これには、情報要求 (文書その他の記録、関連する乙の「担当者」との面談、またはこれらに類似するもの) に対し適時かつ十分に対応することが含まれます。

1.2. 両当事者は、(a) 要求に応じて追加の情報を相互に提供すること、(b) かかるその他の文書を作成し、相互に提供すること、(c) その他の行為および物事を行うことのすべてに合意します。これらはすべて、「本条件」および「本条件」において参照された文書の意図を実行することを目的として他方当事者が合理的に要求することがあります。例として、甲が要求した場合、乙は、「復処理者」および従契約者との書面契約の、プライバシーおよびセキュリティーに関する条件を適時に提供するものとします。これには、乙がその権利を有する場合、契約書自体へのアクセスを認めるなどの方法があります。

1.3. 甲が要求した場合、乙は、「成果物」およびそのコンポーネントが製造、開発その他ソーシングされる国に関する情報を適時に提供するものとします。

2. 検証 (以下で使用される「設備」とは、乙が「Kyndryl 資料」をホストし、処理し、またはこれにアクセスする物理的ロケーションをいいます。)

2.1. 乙は、「本条件」の遵守を証する監査可能な記録を維持するものとします。

2.2. 甲は、自ら、または外部監査人と共に、30「日」前までに乙に通知したうえで、乙による「本条件」の遵守を検証することができます。これには、かかる目的で「設備」にアクセスすることが含まれますが、甲は、乙が「Kyndryl データ」を「処理」するデータ・センターにはアクセスしないものとします。ただし、そうすることによって関連情報が提供される可能性があると甲が判断する誠実な理由がある場合は除きます。乙は、甲による検証に協力するものとします。これには、情報要求 (文書その他の記録、関連する乙の「担当者」との面談、またはこれらに類似するもの) に対し適時かつ十分に対応することが含まれます。乙は、甲が考慮するために、承認済みの行動規範もしくは業界認証を遵守したことの証明を提供するか、または「本条件」を遵守したことを証する情報を提供することができます。

2.3. 次のいずれかの場合を除き、検証は 12 カ月間に 1 回のみ行われるものとします。(a) 12 カ月間中に前回の検証からの懸念事項の乙による修復を甲が検証する。(b) 「セキュリティー侵害」が発生し、当該侵害に関連する義務の遵守を検証することを甲が希望している。いずれの場合も、上記の第 2.2 条に定めるとおり甲は 30「日」前の事前通知を送付しますが、「セキュリティー侵害」に対処する必要性によって、29「日」前までの書面による通知をもって甲が検証を実施することができます。

2.4. 規制当局または「その他の管理者」は、第 2.2 条および第 2.3 条における甲のものと同一の権利を行使することができます。その際、規制当局は法律の下で自らが有する追加の権利を行使することができると理解します。

2.5. 乙が「本条件」のいずれも遵守していないと甲が結論づける合理的な根拠がある場合 (かかる根拠が「本条件」その他に基づく検証から生じたものかは問いません。)、乙は、かかる不遵守を速やかに改善するものとします。

3. 反偽造プログラム

3.1. 乙の「成果物」に電子部品 (例: ハード・ディスク・ドライブ、ソリッド・ステート・ドライブ、メモリー、中央演算処理装置、ロジック・デバイスまたはケーブル) が含まれる場合、乙は、文書化された偽造防止プログラムを維持し、これに従うものとします。かかるプログラムの目的は、まず第一に乙が偽造電子部品を甲に提供することを防止するため、第二に乙が誤って偽造電子部品を甲に提供した場合に速やかに検出し改善するためです。乙は、文書化された偽造防止プログラムを維持し、これに従う義務と同一の義務を、乙の「成果物」に含まれる電子部品を甲に提供する乙のすべての取引先に課すものとします。

4. 修復

4.1. 乙が「本条件」に基づく義務のいずれかに違反し、当該違反により「セキュリティー侵害」が引き起こされた場合、乙は、甲の合理的な指示およびスケジュールで、自らの違反を是正し、かかる「セキュリティー侵害」の悪影響を排除するものとします。ただし、乙がマルチテナントの「ホスト・サービス」を提供したことにより「セキュリティー侵害」が生じ、その結果として Kyndryl を含む乙の多くのお客様が影響を受ける場合、「セキュリティー侵害」の性質により、乙は、適時かつ適切に、自らの不履行を是正し、当該「セキュリティー侵害」の悪影響を排除します。その際、かかる是正および排除に関する Kyndryl の意見について十分に考慮するものとします。

4.2. 甲は、適切または必要であると判断する場合、第 4.1 条で参照される「セキュリティー侵害」の排除に参加する権利を有し、乙は、かかる「セキュリティー侵害」に関して、自らの履行を是正する際の費用、および両当事者に発生する修復費用について負担します。

4.3. 例として、「セキュリティー侵害」に関連する修復費用には、「セキュリティー侵害」の検出および調査、適用法令に基づく責任の決定、侵害に関する通知の送付、コール・センターの設立および維持、クレジット監視およびクレジット・リストア・サービスの提供、データの再ロード、製品の欠陥の改善 (「ソース・コード」その他の開発を通じたものを含みます。)、上記の事項を支援するための第三者の維持、ならびに「セキュリティー侵害」の悪影響を排除するために必要なその他費用などが含まれます。修復費用には、甲の逸失利益、ビジネス機会の損失、価値の損失、逸失収益、信用毀損、節約すべかりし費用は含まれません。