第1条　連絡先個人情報

本条は、サプライヤーまたはキンドリルが他方当事者の連絡先個人情報（BCI）を処理する場合に適用されます。

1.1　キンドリルおよびサプライヤーは、サプライヤーによるサービスおよび成果物の提供に関連するビジネスを行っている限り、他方当事者の BCI を処理することができます。

1.2　一方の当事者は以下をします。

(a)　他のいかなる目的のためにも、他方当事者の BCI を使用または開示しない（明確にすると、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 をマーケティングを目的として販売、使用もしくは開示しない。また、必要に応じて、影響を受けるデータ主体の事前の書面による同意を得る。

(b)　他方当事者が書面で要求する場合、個人情報の不正使用が発生し、その当事者が処理の停止および修正を求める場合はいつでも、他方当事者の BCI の削除、修正、訂正、返却、処理に関する情報の提供、処理の制限、またはその他の合理的に要求された措置を速やかに講じる。

1.3　両当事者は、互いの BCI に関して共同管理者関係を締結しておらず、取引文書のいかなる規定も、共同管理者関係を確立する意図を示すものとして解釈または理解しないでください。

1.4　キンドリルの BCI 処理に関するその他の詳細が記載されているキンドリルのプライバシー・ステートメントは、https://www.kyndryl.com/us/en/privacy でご覧いただけます。

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対策を実施し、今後も維持します。

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侵害に気付いた場合、キンドリルに速やかに（いかなる場合も 48 時間以内に）通知します。サプライヤーは、cyber.incidents@kyndryl.com 宛てに通知を提供します。サプライヤーは、そのような違反やサプライヤーの是正と修復に関する活動の状況に関して、合理的に要求された情報をキンドリルに提供するものとします。例えば、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、管理その他のアクセスを証明するログ、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、これらは侵害またはサプライヤーの修復と回復の作業に関連する範囲に限ります。

1.7　サプライヤーがキンドリルの BCI のみを処理しており、その他のいかなる種類のデータもしくは資料、またはキンドリルの会社システムにアクセスしない場合、その処理には、本条および第 10 条（協力、検証および修復）のみが適用されます。

第2条　技術的および組織的措置、データのセキュリティ

本条は、サプライヤーがキンドリルの BCI 以外のキンドリルのデータを処理する場合に適用されます。サプライヤーは、すべてのサービスと成果物を提供する際に本条の要件を遵守し、そうすることにより、キンドリルのデータを紛失、破壊、改変、偶発的または不正な開示、偶発的または不正なアクセス、および違法な形態の処理から保護します。本条の要件は、サプライヤーが成果物およびサービスを提供する際に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・センター環境を含む）に適用されます。

1.　データの使用

1.1　サプライヤーは、キンドリルから事前の書面による同意を得ることなく、キンドリルのデータに追加したり、キンドリルのデータに個人データを含むその他の情報やデータを含めたりすることはできません。また、サプライヤーは、サービスと成果物を提供する以外の目的で、集計またはその他のいかなる形式であれ、キンドリルのデータを使用することはできません（例えば、サプライヤーは、サプライヤーの提供物の有効性または改善手段の評価、新しい提供物を作成するための研究開発、またはサプライヤーの提供物に関する報告書の生成を目的として、キンドリルのデータを使用または再利用することは許可されていません）。サプライヤーは、取引文書で明示的に許可されている場合を除き、キンドリルのデータを販売することは禁じられています。

1.2　サプライヤーは、取引文書で明示的に許可されている場合を除き、成果物またはサービスの一部として Web 追跡技術（HTML5、ローカル・ストレージ、第三者のタグまたはトークン、Web ビーコンなど）を埋め込みません。

2.　第三者の要求と守秘義務

2.1　サプライヤーは、キンドリルが書面によって事前に許可しない限り、いかなる第三者にもキンドリルのデータを開示しません。政府（規制当局を含む）がキンドリルのデータへのアクセスを要求する場合（米国政府がサプライヤーに対して、キンドリルのデータを取得するよう国家安全保障命令を出す場合など）、またはキンドリルのデータの開示が法律で別途義務付けられている場合、サプライヤーはキンドリルに、その要求もしくは要件を書面で通知し、キンドリルがいかなる開示に対しても異議を申し立てる合理的な機会を得られるようにします（法律によって通知を禁じられている場合、サプライヤーは、裁判その他の手段を通じて、キンドリルのデータの禁止または開示に異議を唱えることが適切であると自身が合理的に判断する措置を講じます）。

2.2　サプライヤーは、キンドリルに対し、(a) サービスまたは成果物を提供するために、キンドリルのデータにアクセスする必要がある、キンドリルの従業員のみがアクセスし、それらのサービスおよび成果物を提供するために必要な範囲でのみアクセスできること、および、(b) 本規約が許可する範囲でのみ、キンドリルのデータを使用および開示することを義務付ける機密保持義務をキンドリルの従業員に課していること、を保証します。

3.　キンドリルのデータの返却または削除

3.1　取引文書の解約もしくは期間満了時、またはキンドリルが要求する場合はそれ以前に、サプライヤーは、キンドリルの選択に従い、キンドリルのデータを削除または返却します。キンドリルが削除を要求する場合、サプライヤーは、業界のベスト・プラクティスに従って、データを読み取れず、再度つなぎ合わせたり、組み立てたりできないようにしたうえで、キンドリルに対し、削除を証明します。キンドリルが、キンドリルのデータの返却を要求する場合、サプライヤーは、キン

ドリルの合理的なスケジュールに従い、かつ、キンドリルの合理的な書面による指示に従って、返却します。

第3条　プライバシー

この条項は、サプライヤーがキンドリルの個人データを処理する場合に適用されます。

1.　処理

1.1　キンドリルは、本規約、取引文書、および両当事者間で締結された関連する基本契約に記載された指示など、キンドリル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、キンドリルの個人データを処理する処理者として、サプライヤーを指名します。サプライヤーが指示に応じない場合、キンドリル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できます。指示がデータ保護法に違反していると判断する場合、サプライヤーは、速やかに、かつ、法で定められた期間内に、キンドリルにその旨を通知します。サプライヤーが本規約の下で負う義務のいずれかを遵守せず、その不履行により、個人情報の不正使用が発生する場合、または一般的に、個人情報の不正使用が発生した場合、キンドリルは、キンドリルの合理的な指示とスケジュールに従って、処理を停止し、不遵守を修正し、不正使用の有害な影響を修復する権利を有します。

1.2　サプライヤーは、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　取引文書の補足文書、または取引文書自体に、キンドリルのデータに関して以下が記載されています。

(a)　データ主体のカテゴリー
(b)　キンドリルの個人データの種類
(c)　データ・アクションと処理アクティビティー
(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　サプライヤーは、第 2 条（技術的および組織的措置、データのセキュリティ）ならびに第 8 条（技術的および組織的措置、一般的なセキュリティ）に定められた技術的および組織的措置を実施および維持し、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のレベルを確保します。サプライヤーは、第 2 条、第 3 条、および第 8 条の制限を認め、理解し、それらに従います。

3.　データ主体の権利と要求

3.1　キンドリルの個人データに関するデータ主体の権利（データの修正、削除、またはブロックなど）を行使することをデータ主体が要求する場合、サプライヤーは速やかに（キンドリルおよびその他の管理者が法的義務を履行できるスケジュールで）キンドリルに通知します。サプライヤーはまた、データ主体がキンドリルにそのような要求をするように直ちに指示することもできます。サプライヤーは、法的に必要であるか、キンドリルからの書面による指示がない限り、データ主体からのいかなる要求にも応じません。

3.2　キンドリルが、キンドリルの個人データに関する情報を他の管理者または他の第三者（データ主体または規制当局など）に提供する義務を負う場合、サプライヤーは、キンドリルがそのようなその他の管理者または第三者に適時に対応できるスケジュールで、情報を提供し、キンドリルが要求するその他の合理的な措置を講じることによって、キンドリルを支援します。

4. 復処理者

4.1 サプライヤーは、新規の復処理者を追加する前に、または既存の復処理者による処理の範囲を拡大する前に、キンドリルに事前に書面で通知し、このような書面による通知で、復処理者の名前を特定し、処理の新しい範囲または拡大された範囲を説明します。キンドリルは、前記の新規の復処理者または拡大された範囲について、合理的な根拠に基づき随時、異議を唱えることができます。その場合、両当事者は、誠意を持って協力し、キンドリルの異議に対処します。随時異議を申し立てられるキンドリルの権利を条件として、サプライヤーは、新規の復処理者に委託し、または既存の復処理者による処理の範囲を拡大することができます。ただし、キンドリルがサプライヤーの書面による通知を受領してから 30 日以内に異議を提起しない場合に限ります。

4.2 サプライヤーは、復処理者がキンドリルのデータを処理する前に、承認を受けた各復処理者に対して、本規約に定められるデータ保護、セキュリティ、証明書の取得義務を課します。サプライヤーは、各復処理者の義務の履行について、キンドリルに対して全責任を負います。

5. 域外でのデータ処理

以下で使用される用語は、以下の意味を有します。

「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従って、関連する転送に関して適切なレベルのデータ保護を提供する国を意味します。

「データ輸入者」とは、十分国で設立されていない処理者または復処理者を意味します。

「EU 標準契約条項」（EU Standard Contractual Clauses、以下「EU SCC」）とは、EU 標準契約条項（委員会決定 2021/914）を意味し、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ます。同条項は https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en で公開されています。

「セルビア標準契約条項」（Serbian Standard Contractual Clauses、以下「セルビア SCC」）とは、Serbian Commissioner for Information of Public Importance and Personal Data Protection で採用されているセルビア標準契約条項を意味します。同条項は、https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx で公開されています。

「標準契約条項」（以下「**SCC**」）とは、十分国で設立されていない処理者への個人データの転送について、適用データ保護法により要求される契約条項を意味します。

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付随する英国の国際データ転送に関する補遺を意味し、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意味します。

5.1　サプライヤーは、キンドリルから事前の書面による同意を得ることなく、キンドリルの個人データを国境を越えて（リモート・アクセスによる場合も含め）転送または開示しません。キンドリルがそのような同意をする場合、両当事者は、適用されるデータ保護法を確実に遵守するために協力します。これらの法律でソース・コード・コントロール・システム（SCC）が求められる場合、サプライヤーはキンドリルの要求があり次第、速やかに SCC を締結します。

5.2　EU SCC について：

(a)　サプライヤーが十分国で設立されていない場合：サプライヤーは本規約により、データ輸入者としてキンドリルと EU SCC を締結します。また、サプライヤーは EU SCC 第 9 条に従って、承認済みの各復処理者と書面による契約を締結し、要求された場合は、これらの契約書の写しをキンドリルに提供します。

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

(ii) EU SCC のモジュール 2 は、キンドリルが管理者である場合に適用され、キンドリル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 加盟国の裁判所で解決されることに合意します。その法律が(1)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) 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します。

(b)　サプライヤーとキンドリルの両当事者が十分国で設立されている場合、サプライヤーはデータ輸出者として、非十分国で承認された各復処理者と EU SCC を締結します。サプライヤーは、必要な移転影響評価（TIA）を実施し、(1) 補足措置を適用する必要がある場合、および (2) 適用された措置について、遅滞なくキンドリルに通知します。要求される場合、サプライヤーは TIA の結果と、結果を理解して評価するために必要な情報をキンドリルに提供します。キンドリルがサプライヤーの TIA の結果または適用された補足措置に同意しない場合、キンドリルとサプライヤーは協力して実行可能な解決策を見つけます。キンドリルは、関係するサプライヤーのサービスを補償なしで一時停止または終了する権利を保持します。疑義を避けるために付言すると、これは、以下の第 5.2 条(d)項で概要を示すように、サプライヤーの復処理者がキンドリルまたはそのお客様との EU SCC の当事者になる義務を免除するものではありません。

(c)　サプライヤーが欧州経済地域で設立され、キンドリルが一般データ保護規則 2016/679 の対象とならない管理者である場合は、EU SCC のモジュール 4 が適用され、サプライヤーはこれにより、キンドリルのデータ輸出者として 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であること、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ことに同意します。

(d)　その他の管理者（お客様または関連会社など）が第 7 条の「ドッキング条項」に関連する EU SCC の当事者になることを要求する場合、サプライヤーは本規約によりかかる要求に同意します。

(e)　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は、本規約、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。

(f) EU SCC と本規約の間に矛盾がある場合、EU SCC が優先されます。

5.3 英国補足契約書について：

(a) サプライヤー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) サプライヤーは、キンドリルを輸入者として「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) サプライヤーは、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キンドリルに提出するものとします。

(b) サプライヤーが十分国で設立され、キンドリル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、サプライヤーは、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、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」について：

(a) サプライヤーが十分国で設立されていない場合、(i) サプライヤーは、本規約により、サプライヤー自身のために処理者としてキンドリルとセルビア SCC を締結し、(ii) サプライヤーは、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で契約を締結し、要求された場合は、その契約の写しをキンドリルに提供します。

(b) サプライヤーが十分国で設立されている場合、サプライヤーは非十分国に所在する各復処理者のためにキンドリルとセルビア SCC を締結します。サプライヤー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、サプライヤーは、復処理者にキンドリルの個人データ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 をキンドリルに提供し、キンドリルが副署できるようにします。

(c) キンドリルとサプライヤーの間のセルビア SCC は、事実に応じて、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」間の同一の（back to back）書面による契約のいずれかとして機能します。セルビア SCC と本規約の間に矛盾がある場合、セルビア SCC が優先されます。

(d) 非十分国への個人データの転送を管理する目的で、セルビア SCC の付録 1 から 8 を完了するために必要な情報は、本規約、取引文書の別紙、または取引文書自体に記載されています。

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条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.　支援と記録

6.1　サプライヤーは、処理の性質を考慮して、データ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、キンドリルを支援します。サプライヤーは、自身が入手可能な情報を考慮して、処理のセキュリティ、セキュリティ侵害の通知と連絡、およびデータ保護に関する影響評価の作成 に関する義務の遵守を確実にするために、キンドリルを支援します（必要に応じて、担当する規制当局との事前協議を含みます）。

6.2　サプライヤーは、各復処理者（各復処理者の代表者とデータ保護担当者を含む）の名前および連絡先の詳細に関する最新の記録を保持します。要求された場合、サプライヤーは、キンドリルがお客様またはその他の第三者からの要求に適時に対応できるスケジュールで、この記録をキンドリルに提供します。

第4条　技術的および組織的措置、コードのセキュリティ

本条は、サプライヤーがキンドリルのソース・コードにアクセスする場合に適用されます。サプライヤーは、本条の要件に従い、それにより、キンドリルのソース・コードを喪失、破壊、改変、偶発的または不正な開示、偶発的または不正なアクセス、違法な形態の処理から保護します。本条の要件は、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む、成果物およびサービスの提供、およびキンドリルのテクノロジーの取り扱いにおいてサプライヤーが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に適用されます。

1.　セキュリティ要件

以下で使用される用語は、以下の意味を有します。

「禁止国」とは、(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）」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（U.S. National Defense Authorization Act of 2019）第 1654 条に記載されている国、または(c) 取引文書において「禁止国」として特定されている国、を意味します。

1.1　サプライヤーは、第三者の利益に資するエスクローにキンドリルのソース・コードを配布せず、または置かないものとします。

1.2　サプライヤーは、禁止国に配置されているサーバーにキンドリルのソース・コードを置かないものとします。サプライヤーは、禁止国に所在している、または禁止国を訪問している（該当する訪問中）いかなる者（自身の人材を含む）にも、理由の如何を問わず、キンドリルのソース・コードが世界中のどこに配置されているかにかかわらず、キンドリルのソース・コードへのアクセスまたは使用を許可しません。また、サプライヤーは、禁止国でそのようなアクセスまたは使用を必要とする開発、テスト、またはその他の作業を行うことを許可しません。

1.3　サプライヤーは、法律または法解釈によりキンドリルのソース・コードを第三者に開示することが要求される法域にキンドリルのソース・コード」を置かず、また配布しません。キンドリルのソース・コードが配置されている法域において法または法解釈が変更され、これによりサプライヤーがかかるキンドリルのソース・コードを第三者に開示する必要が生じる可能性がある場合、サプライヤーは、かかるキンドリルのソース・コードを直ちに破壊するか、その法域から直ちに撤去します。また、その法または法解釈が引き続き効力を有する場合、その法域にその他のキンドリルのソース・コードを配置しません。

1.4　サプライヤーは、サプライヤー、キンドリルまたはいずれかの第三者が 2019 年米国国防権限法第 1654 条または第 1655 条に基づく開示義務を負う原因となる行動（契約の締結を含む）を直接または間接的に取らないものとします。明確にすると、両当事者間の取引文書または関連する基本契約で明示的に許可されている場合を除き、サプライヤーは、いかなる状況でも、キンドリルから事前の書面による同意を得ることなく、キンドリルのソース・コードを第三者に開示することは許可されていません。

1.5　キンドリルがサプライヤーに対し、または第三者がいずれかの当事者に対し、(a) 禁止国または上記第1.3条が適用される法域にサプライヤーがキンドリルのソース・コードを持ち込むことを許可したこと、(b) 両当事者間の取引文書または関連する基本契約またはその他の契約で許可されていない方法でサプライヤーがキンドリルのソース・コードをリリース、アクセスまたは使用したこと、(c) サプライヤーが上記第 1.4 項に違反したことのいずれかを通知した場合、コモン・ロー、衡平法上、または取引文書、関連する基本契約、または当事者間のその他の合意の不履行に対処する

キンドリルの権利を制限することなく、(i) そのような通知がサプライヤーに対するものである場合、サプライヤーは速やかにその通知をキンドリルと共有し、(ii) サプライヤーは、キンドリルの合理的な指示により、キンドリルが合理的に決定するスケジュールに従ってその問題を調査し、（サプライヤーとの協議の後に）是正します。

1.6　キンドリルが、サイバー・セキュリティ、知的財産の盗難、あるいはそれに類似または関連するリスク（そのような変更がなければ、キンドリルが特定のお客様や特定の市場への販売を制限されたり、お客様のセキュリティまたはサプライチェーンの要件を満たすことができなくなったりするリスクを含む）に対処するために、ソース・コードへのアクセスに関するサプライヤーのポリシー、手続き、管理、または慣行の変更が必要であると合理的に判断する場合、キンドリルはサプライヤーに連絡して、そのようなポリシー、手続き、管理、または慣行の変更など、そのようなリスクに対処するために必要な措置について話し合うことができます。 キンドリルが要求する場合、サプライヤーはキンドリルと協力して、そのような変更が必要かどうかを評価し、相互に合意した適切な変更を実施します。

第5条　セキュアな開発

本条は、サプライヤーが自らの、もしくは第三者のソース・コードやオンプレミス・ソフトウェアをキンドリルに提供する場合、または、サプライヤーのいずれかの成果物もしくはサービスがキンドリルの製品やサービスの一部としてキンドリルのお客様に提供される場合に適用されます。

1.　セキュリティの即応性

1.1　サプライヤーは、サプライヤーのいずれかの成果物に依拠するキンドリルの製品およびサービスのセキュリティ準備状況を評価するキンドリルの内部プロセスに協力します。これには、文書その他の記録、関連するサプライヤーの担当者との面談、またはこれらに類似するものを通じた情報の要求に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、サプライヤーがキンドリルにオンプレミス・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　サプライヤーは、取引文書の期間を通じて、業界ベスト・プラクティスに従って、(a) サプライヤーまたはサプライヤーが関与する第三者が、成果物のために、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開発、構築、テスト、運用システムと環境を保護し、および (b) 喪失、違法な形態の取り扱い、不正なアクセス、開示または改ざんからすべての成果物のソース・コードを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、物理インフラストラクチャー、インシデント対応、および人員に重点を置いたセキュリティ・ポリシー、手続き、制御を実装し、実施します。

3.　ISO 20243 認証

3.1　本第 3 条は、サプライヤーの成果物またはサービスのいずれかが、キンドリルの製品またはサービスの一部としてキンドリルのお客様に提供される場合にのみ適用されます。

3.2　サプライヤーは、ISO 20243、情報技術、Open Trusted Technology Provider、TM 標準（O-TTPS）、悪意を持って汚染された製品および偽造製品の軽減に準拠しているという証明書を取得し

ます（自己評価による証明書、または有名な独立監査法人の評価に基づく証明書のいずれか）。あるいは、サプライヤーが書面で要求し、キンドリルが書面で承認する場合、サプライヤーは、セキュアな開発とサプライ・チェーンの慣行に対処する実質的に同等の業界標準に準拠する証明書を取得します（キンドリルが承認する場合は、キンドリルが承認するとおりに、自己評価による証明書、または有名な独立監査法人の評価に基づく証明書のいずれか）。

3.3　サプライヤーは、取引文書の発効日から 180 日以内に、ISO 20243 または（キンドリルが書面で承認する場合）実質的に同等の業界標準に準拠する証明書を取得し、その後 12 か月ごとに当該証明書を更新します（各更新時に、適用される標準のその時点の最新バージョン（ISO 20243）、またはキンドリルが書面で承認する場合は、セキュアな開発とサプライチェーンの慣行に対応する実質的に同等の業界標準の準拠を証明します）。

3.4　サプライヤーは、要求された場合、上記の第 2.1 条および第 2.2 条に従って、サプライヤーが取得する義務を負う証明書の写しをキンドリルに速やかに提供します。

4.　セキュリティの脆弱性

以下で使用される用語は、以下の意味を有します。

「エラーの訂正」とは、成果物のセキュリティの脆弱性を含む、エラーまたは欠陥を修正するバグの修正と改訂を意味します。

「軽減策」とは、セキュリティの脆弱性リスクを軽減または回避する既知の手段を意味します。

「セキュリティの脆弱性」とは、何者かによる攻撃を可能にする成果物の設計、コーディング、開発、実装、テスト、運用、サポート、保守または管理の状態で、不正アクセスまたは利用につながる可能性のあるものを意味し、(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、などが含まれます。共通脆弱性識別子（CVE）の ID、または評価あるいは正式な分類の割り当てにかかわらず、セキュリティの脆弱性は存在することがあります。

4.1　サプライヤーは、自らが、(a) 業界のベスト・プラクティスを使用し、継続的な静的および動的ソース・コード・アプリケーションのセキュリティ・スキャン、オープン・ソース・セキュリティ・スキャン、システム脆弱性スキャンなどを通してセキュリティの脆弱性を特定すること、(b) 本規約の要件を遵守して、成果物のみならず、サプライヤーがサービスと成果物を作成して提供するすべての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の脆弱性の予防、検出、および訂正に役立てることを、表明し、保証します。

4.2　サプライヤーが成果物やITアプリケーション、プラットフォーム、またはインフラストラクチャーにあるセキュリティの脆弱性に気付いた場合、サプライヤーは、下表で定義された重大度レベルと時間枠に従って、成果物のすべてのバージョンとリリースに対してエラーの訂正と軽減策をキンドリルに提供します。

重大度*
緊急のセキュリティの脆弱性 – 重大で潜在的にグローバルな脅威を構成するセキュリティの脆弱性です。キンドリルは、CVSS基本値に関係なく、独自の裁量で緊急のセキュリティの脆弱性を指定します。
重大 – CVSS 基本値が 9 ～10.0 のセキュリティ脆弱性
高 – CVSS基本値が7.0 ～8.9のセキュリティ脆弱性

中 – CVSS 基本値が 4.0 ～6.9 のセキュリティ脆弱性
低 – CVSS 基本値が 0.0 ～3.9 のセキュリティ脆弱性

時間枠				
緊急	***重大***	***高***	***中***	***低***
キンドリルの最高情報セキュリティオフィス責任者の判断に従い、4 日以内	30 日	30 日	90 日	業界のベスト・プラクティスに従う

*セキュリティの脆弱性に CVSS 基本値が容易に割り当てられない場合、サプライヤーは、そのような脆弱性の性質と状況に適した重大度レベルを適用します。

4.3　公開されているセキュリティの脆弱性のうち、サプライヤーがキンドリルにエラーの訂正または軽減策を提供していないものについては、サプライヤーは、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管理を実装します。

4.4　キンドリルが、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の脆弱性に対するサプライヤーの対応に満足しない場合、サプライヤーは、キンドリルの他のいずれの権利にも不利益を与えることなく、サプライヤーの統括責任者、またはエラーの訂正の実行者に相当する担当役員とキンドリルが懸念事項について直接協議できるよう、キンドリルのために速やかに調整します。

4.5　セキュリティの脆弱性の例として、セキュリティ修正プログラムが提供されなくなっている第三者のコードや、サービスを終了した（EOS）オープン・ソース・コードが該当します。

第6条　会社システムへのアクセス

本条は、サプライヤーの従業員が会社システムにアクセスできる場合に適用されます。

1.　　総則

1.1　　キンドリルは、サプライヤーの従業員に会社システムへのアクセスを承認するかどうかを決定します。キンドリルが承認する場合、サプライヤーは、アクセス権を持つ従業員に本条の要件を遵守させます。

1.2　　キンドリルは、サプライヤーの従業員が会社システムにアクセスする手段を特定します。これには、その従業員がキンドリルまたはサプライヤーが提供するデバイスを通じて会社システムにアクセスするかどうかも含まれます。

1.3　　サプライヤーの従業員は、サービスを提供するために、会社システムにのみアクセスでき、キンドリルがアクセスを承認するデバイスのみを使用できます。サプライヤーの従業員は、キンドリルが承認するデバイスを使用して、その他の個人やエンティティにサービスを提供したり、本サービスのために、または本サービスに関連して、サプライヤーまたは第三者の 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・ツールもしくはそれに相当するものにアクセスすることはできません。

1.4　　明確にすると、サプライヤーの従業員は、キンドリルが会社システムへのアクセスを許可したデバイスを私的な理由で使用することはできません（サプライヤーの従業員は、音楽、動画、写真その他同様のアイテムなどの個人ファイルをそのようなデバイスに保存してはならず、また、私的な理由で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　　サプライヤーの従業員は、キンドリルから事前に書面による承認を得ることなく、会社システムからアクセス可能なキンドリル資料を複製してはなりません（また、いかなるキンドリル資料も、USB、外付けハード・ドライブ、その他の携帯型ストレージ・デバイスに絶対に複製しないでください）。

1.6　　サプライヤーは、要求された場合、従業員の名前によって、キンドリルが特定する期間のいずれかの時点で、その従業員がアクセスを許可されていて、アクセスした会社システムを確認します。

1.7　　サプライヤーは、会社システムにアクセスするサプライヤーの従業員が、(a) サプライヤーに雇用されなくなった、または(b) そのようなアクセスを必要とする業務に従事しなくなった場合、24 時間以内にキンドリルに通知します。サプライヤーはキンドリルと協力して、そのような元従業員または現在の従業員のアクセス権限を直ちに取り消します。

1.8　　サプライヤーは、セキュリティ・インシデント（キンドリルもしくはサプライヤーのデバイスの紛失、またはデバイス、データ、資料その他あらゆる種類の情報に対する不正アクセスなど）が実際に生じた場合、またはその疑いがある場合、直ちにキンドリルに報告し、そのインシデントの調査においてキンドリルと協力します。

1.9　　サプライヤーは、キリンドルから事前の書面による同意を得ることなく、代理人、独立した請負業者または従契約者の従業員に、会社システムへのアクセスを許可することはできません。キンドリルがかかる同意をする場合、サプライヤーは、これらの者とその雇用主を契約によって拘束し、あたかもサプライヤーの従業員であるかのように、本条の要件を遵守させます。また、これら

の者によるかかる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は、サプライヤーがキンドリル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 サプライヤーは従業員に対し、会社システムへのアクセスを安全な方法で促進するためにキンドリルが必要と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に指示します。サプライヤーもその従業員も、そのソフトウェアの操作またはソフトウェアが有効にするセキュリティ機能に干渉しないものとします。

2.2 サプライヤーとその従業員は、キンドリルが設定するデバイス構成規則を遵守するか、キンドリルが意図するとおりにソフトウェアが確実に機能するようにキンドリルと協力します。例えば、サプライヤーは、ソフトウェア Web サイトのブロックや自動パッチ機能を無効にしません。

2.3 サプライヤーの従業員は、会社システムへのアクセスに使用するデバイス、デバイスのユーザー名、パスワードなどを他の人と共有することはできません。

2.4 キンドリルがサプライヤーの従業員にサプライヤー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許可する場合、サプライヤーは、キンドリルが承認するデバイスにオペレーティング・システムをインストールして実行し、そのオペレーティング・システムを、キンドリルが指示した後妥当な時間内に新規バージョン、または新しいオペレーティング・システムにアップグレードします。

3. 監督と協力

3.1 キンドリルは、サプライヤーまたはサプライヤーの従業員などに事前に通知することなく、潜在的な侵入およびその他のサイバー・セキュリティの脅威を、キンドリルが必要または適切であると考える手段を使用して、いかなる方法でも監視および修復する無条件の権利を有します。例えば、キンドリルは、随時、(a) あらゆるデバイスへのセキュリティ・テストの実施、(b) デバイスに保存されている、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む）、記録、ファイルその他のアイテムのモニタリング、技術的その他の手段を通じた復旧、レビュー、および(c) あらゆるデバイスの完全な法的証拠となる画像の取得を実行することができます。キンドリルが自らの権利を行使するためにサプライヤーの協力を必要とする場合、サプライヤーは、キンドリルからのこのような協力の要請に完全かつ適時に応えます（例えば、任意のデバイスを安全に構成する、任意のデバイスに監視またはその他のソフトウェアをインストールする、システム・レベルの接続の詳細を共有する、任意のデバイスでインシデント対応措置を講じる、完全な法的証拠となる画像を取得するためにキンドリルが任意のデバイスに物理的にアクセスできるようにする、などの要求とそれに関連する要求などがあります）。

3.2 キンドリルは、キンドリルを保護するために必要であると判断した場合、サプライヤーまたはサプライヤーの従業員などに事前に通知することなく、いつでも、サプライヤーの特定の従業員またはすべての従業員の会社システムへのアクセスを取り消すことができます。

3.3 ある種のデータ、資料、またはその他の情報が一部の場所または複数の場所にのみ存在することを要求する規定や、一部の場所または複数の場所の人物のみがそのようなデータ、資料またはその他の情報にアクセスすることを要求する規定など、キンドリルの権利は、いかなる点でも、取引文書の規定、両当事者間の関連する基本合意、または両当事者間のその他の合意によって、阻止、軽減、制限されることはありません。

4. キンドリルのデバイス

4.1　　キンドリルはすべてのキンドリルのデバイスの所有権を保持し、サプライヤーは、盗難、破壊行為、過失などによるデバイス紛失のリスクを負います。サプライヤーは、キンドリルから事前の書面による同意を得ることなく、キンドリルのデバイスに変更を加えたり、変更の許可を与えたりないものとします。これらの変更には、デバイス、ソフトウェア、アプリケーション、セキュリティ設計、セキュリティ構成、または物理的、機械的、または電気的な設計に対する変更である改変が含まれます。

4.2　　サプライヤーは、サービスを提供するためにキンドリルのデバイスが必要でなくなった後 5 営業日以内に、すべてのデバイスを返却します。また、キンドリルが要求する場合、同時に、これらのデバイス上のすべてのデータ、資料、およびその他の情報を業界のベスト・プラクティスに従い、データ、資料、およびその他の情報をすべて永久に消去し、コピーを保持せずに、すべて破棄します。キンドリルのデバイス・サプライヤーは、キンドリルのデバイスを、サプライヤーに引き渡した時と同様の状態で（通常の損耗を除きます）、費用を自己負担して、梱包し、キンドリルが指定する場所に返却します。サプライヤーが本第 4.2 条におけるいずれかの義務を遵守しなかった場合、会社システムへのアクセスがその契約に基づくサプライヤーの作業またはその他の活動を円滑にしている場合、その契約は「関連する」との理解の下で、その不履行は取引文書とその関連基本契約、および当事者間のあらゆる関連契約に対する重大な違反を構成することになります。

4.3　　キンドリルは、キンドリルのデバイスのサポート（デバイスの検査、予防的および修復的な保守など）を提供します。サプライヤーは、キンドリルに修復サービスの必要性を速やかに通知します。

4.4.　　キンドリルが所有する、またはライセンスを付与する権利を有するソフトウェア・プログラムについて、キンドリルはサプライヤーに対し、キンドリルのデバイスの許可された使用をサポートするため、使用、保存、および十分な数量を複製する一時的な権利を付与します。サプライヤーは、適用法によって明示的に許可されている場合を除き、契約上の権利放棄の可能性なしに、プログラムの他人への譲渡、ソフトウェア・ライセンス情報の複製、逆アセンブル、逆コンパイル、リバース・エンジニアリング、またはその他の方法によるプログラムの翻訳はできません。

5.　　更新

5.1　　取引文書または当事者間の関連基本契約に矛盾する規定がある場合でも、サプライヤーに書面で通知することにより、サプライヤーの同意を得る必要なく、キンドリルは、適用法やお客様の義務に基づく要件に対応するために、セキュリティのベスト・プラクティスの進展を反映するために、または会社システムまたはキンドリルを保護するためにキンドリルが必要と考えるその他の方法で、本条を更新、補足、修正することがあります。

第7条　人材の増強

本条は、サプライヤーの従業員が勤務時間のすべてをキンドリルのためにサービスを提供することに専念し、それらのサービスのすべてをキンドリルの施設、お客様の施設、または自宅から実行し、会社システムにアクセスするためにキンドリルのデバイスを使用するサービスのみを提供する場合に適用されます。

1.　会社システムへのアクセス、キンドリルの環境

1.1　サプライヤーは、キンドリル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によってのみ、サービスを実行できます。

1.2　サプライヤーは、会社システムへのすべてのアクセスについて、第6条（会社システムへのアクセス）に規定する条項を遵守します。

1.3　キンドリルが提供するデバイスは、サプライヤーとその従業員がサービスを提供するために使用できる唯一のデバイスであり、サプライヤーとその従業員のみがサービスを提供するために使用できます。明確にすると、サプライヤーまたはその従業員は、サービスを提供するために他のデバイスを使用したり、他のサプライヤーのお客様のためにキンドリルのデバイスを使用したり、キンドリルにサービスを提供する以外の目的で使用したりすることはできません。

1.4　キンドリルのデバイスを使用するサプライヤーの従業員は、キンドリル資料を相互に共有し、そのような資料をキンドリルのデバイスに保存することができますが、そのような共有と保存はサービスを正常に実行するために必要な範囲に限定されます。

1.5　サプライヤーまたはその従業員は、キンドリルのデバイス内に保管する場合を除き、いかなる場合も、キンドリルが保持しているキンドリルのリポジトリー、環境、ツール、またはインフラストラクチャーからキンドリル資料を削除することはできません。

1.6　明確にすると、サプライヤーとその従業員は、キンドリルの事前の書面による同意を得ることなく、キンドリル資料をサプライヤーのリポジトリー、環境、ツール、インフラストラクチャー、またはその他のサプライヤーのシステム、プラットフォーム、ネットワークなどに転送することは許可されていません。

1.7　サプライヤーの従業員が勤務時間のすべてをキンドリルのためにサービスを提供することに専念し、それらのサービスのすべてをキンドリルの施設、お客様の施設、または自宅から実行し、会社システムにアクセスするためにキンドリルのデバイスを使用するサービスのみを提供する場合、第8条（技術的および組織的措置、一般的なセキュリティ）はサプライヤーのサービスに適用されません。それ以外の場合は、第8条がサプライヤー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、一般的なセキュリティ

本条は、サプライヤーがサービスまたは成果物をキンドリルに提供する場合に適用されます。ただし、サプライヤーがそれらのサービスおよび成果物を提供する際にキンドリルのBCIに対してのみアクセスする場合（サプライヤーは、他のキンドリルのデータを処理しない、または他のキンドリル資料や会社システムにアクセスしない）、サプライヤーの唯一のサービスおよび成果物がオンプレミス・ソフトウェアをキンドリルに提供することである場合、またはサプライヤーがそのすべてのサービスおよび成果物を第 7 条（第 1.7 条を含む）に従って人材の増強モデルで提供する場合を除きます。

サプライヤーは、本条の要件を遵守し、そうすることによって、(a) キンドリル資料を喪失、破壊、変更、偶発的または不正な開示、および偶発的または不正なアクセスから、(b) キンドリルのデータを違法な形態の処理から、(c) キンドリルのテクノロジーを違法な形態の取り扱いから保護します。本条の要件は、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む、成果物およびサービスの提供、およびキンドリルのテクノロジーの取り扱いにおいてサプライヤーが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に適用されます。

1.　セキュリティ・ポリシー

1.1　サプライヤーは、サプライヤーの業務に不可欠で、すべてのサプライヤーの担当者が遵守しなければならない、業界のベスト・プラクティスに合致する IT セキュリティに関するポリシーと慣行を実施し、それに従います。

1.2　サプライヤーは、少なくとも年に 1 回、IT セキュリティ・ポリシーと慣行を見直し、キンドリル資料を保護するために必要であるとサプライヤーが判断する場合、それらを修正します。

1.3　サプライヤーは、すべての新規従業員の採用に対して標準かつ必須の雇用確認要件を実施し、それを遵守し、さらに、その要件をすべてのサプライヤーの担当者とサプライヤーの完全所有子会社にも適用します。これらの要件には、現地の法律で許可されている範囲の犯罪歴の確認、身元確認の証明、およびサプライヤーが必要と考える追加の確認が含まれます。サプライヤーは、必要であると考える場合、これらの要件を定期的に繰り返し、再検証します。

1.4　サプライヤーは、毎年その従業員にセキュリティとプライバシーに関する研修を提供し、サプライヤーの行動規範または同様の文書に規定されているとおりに、サプライヤーの倫理的な行動規範、機密保持、セキュリティ・ポリシーを遵守することを毎年証明することを従業員全員に要求します。サプライヤーは、サービス、成果物、またはキンドリル資料のいずれかのコンポーネントに管理上アクセスする人物に、追加のポリシーとプロセスに関する研修を提供します。その研修は、各自の職務に固有で、サービス、成果物、およびキンドリル資料を補強し、必要なコンプライアンスと証明を実施するために行われます。

1.5　サプライヤーは、すべてのサービスと成果物、およびキンドリルのテクノロジーのすべての取り扱いについて、意図されたセキュリティとプライバシー、セキュアなエンジニアリング、セキュアな運用を求めるポリシーと手続きの実装、保守、それらの遵守を通じてなど、キンドリル資料の利用可能性を保護および維持するためのセキュリティおよびプライバシー対策を設計します。

2.　セキュリティ・インシデント

2.1　サプライヤーは、コンピューターのセキュリティ・インシデント処理に関する業界のベスト・プラクティスに沿って文書化したインシデント対応ポリシーを実施し、それに従います。

2.2　サプライヤーは、キンドリル資料の不正アクセスや不正使用を調査し、適切な対応計画を定義して実行します。

2.3　サプライヤーは、セキュリティ侵害を認識した場合、キンドリルに迅速に（いかなる場合も 48 時間以内に）通知します。サプライヤーは、cyber.incidents@kyndryl.com 宛てに通知を提供しま

す。サプライヤーは、そのような違反やサプライヤーの是正と修復に関する活動の状況に関して、合理的に要求された情報をキンドリルに提供するものとします。例えば、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、管理その他のアクセスを証明するログ、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、これらは侵害またはサプライヤーの修復と回復の作業に関連する範囲に限ります。

2.4　サプライヤーは、セキュリティ侵害に関連して、キンドリル、キンドリルの関連会社、およびお客様（そのお客様と関連会社を含む）の法的義務（規制当局またはデータ主体に通知する義務を含む）を満たすために、合理的な支援をキンドリルに提供するものとします。

2.5　サプライヤーは、キンドリルが書面で承認する場合、または法律によって義務付けられている場合を除き、キンドリルまたはキンドリル資料に直接的または間接的に関連するセキュリティ侵害について、第三者に報告または通知しないものとします。サプライヤーが第三者に法的に通知を送付する必要があり、それがキンドリルの識別情報を直接的または間接的に公開する場合、サプライヤーはキンドリルに書面で通知します。

2.6　サプライヤーが本規約に基づく義務に違反したことによりセキュリティ侵害が発生する場合、以下が適用されます。

(a)　サプライヤーは、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、報道機関（適用法により義務付けられている場合）、データ主体、お客様その他の者に対して、セキュリティ侵害の通知を提供する際は、自らに発生する費用およびキンドリルに発生する実費を負担します。

(b)　キンドリルが要求する場合、サプライヤーは、データ主体からのセキュリティ侵害に関する質問に回答するために、自ら費用を負担してコール・センターを設立し、その後、当該データ主体がセキュリティ侵害の通知を受けた日付から 1 年間、または適用される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の間、実施します。キンドリルとサプライヤーは、コール・センターの担当者が問い合わせに対応する際に使用するスクリプトやその他の資料を作成するために協力します。あるいは、キンドリルはサプライヤーに対し書面で通知することにより、サプライヤーにコール・センターを設立させる代わりに、自身のコール・センターを設立し、維持することができます。その場合、サプライヤーは、キンドリルがそのコール・センターを設立および維持するために負担した実費をキンドリルに弁済します。

(c)　サプライヤーは、そのようなサービスへの登録を選択し、侵害の影響を受けた個人がセキュリティ侵害についての通知を受けた日から 1 年間、または、適用されるいずれかのデータ保護法が求める期間、キンドリルが信用のモニタリングと信用回復のためのサービスを提供するにあたって負担する実費をキンドリルに弁済します。

3.　物理的セキュリティと入退室管理（以下で使用される「施設」とは、サプライヤーがキンドリル資料をホスト、処理、またはその他の方法でアクセスする物理的な場所を意味します）。

3.1　サプライヤーは、施設への不正な立ち入りを防ぐために、障害物、入口のカード制御、監視カメラ、有人受付デスクなど、適切な物理的入退室管理を実施します。

3.2　サプライヤーが施設および施設内の管理区域にアクセスする場合（一時的なアクセスを含む）は、正式な承認を必要とし、職務および業務上の必要性により制限付きでアクセスします。サプライヤーが一時的なアクセスを許可する場合、訪問者が施設および管理区域にいる間、許可された従業員が付き添います。

3.3　　サプライヤーは、施設内の管理区域への立ち入りを適切に制限するために、業界のベスト・プラクティスに準拠した、多要素アクセス制御を含む物理的なアクセス制御を実装し、すべての立ち入りの試みを記録し、そのログを最低 1 年間保持します。

3.4　　サプライヤーは、(a) 許可されたサプライヤーの従業員が離職する場合、または(b) 許可されたサプライヤーの従業員がアクセスする正当な業務上の必要性を失った場合、施設および施設内の管理区域へのアクセスを取り消すものとします。サプライヤーは、アクセス管理リストから迅速に削除し、物理的なアクセス許可証の返納など、文書化された正式な削除手順に従うものとします。

3.5　　サプライヤーは、周囲の極端な温度、火災、洪水、湿気、盗難、破壊行為など、自然発生および人為的な環境面の脅威から、サービスと成果物、およびキンドリルの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保護するための予防措置を講じます。

4.　　アクセス、介入、移送、分離管理

4.1　　サプライヤーは、サービスの運用、成果物の提供、およびキンドリルのテクノロジーの取り扱いを管理する、文書化されたネットワークのセキュリティ・アーキテクチャーを維持します。 サプライヤーは、そのネットワーク・アーキテクチャーを個別に確認し、システム、アプリケーション、およびネットワーク・デバイスへの不正なネットワーク接続を防止する手段を採用し、安全なセグメンテーション、分離、および多層防御の標準に準拠します。サプライヤーは、ホスティング・サービスのホスティングおよび運用に無線技術を使用してはなりません。それ以外の場合では、サプライヤーは、サービスと成果物の提供、およびキンドリルのテクノロジーの取り扱いにおいて無線ネットワーキング・テクノロジーを使用することができますが、サプライヤーは、そのような無線ネットワークの暗号化と安全な認証が必要です。

4.2　　サプライヤーは、キンドリル資料を論理的に分離し、許可されていない人への開示や、そうした人による利用を防止するために設計された措置を実施します。さらに、サプライヤーは、その実稼働環境、非実稼働環境、およびその他の環境を適切に分離し、キンドリル資料が非実稼働環境内に既に存在するか、非実稼働環境に転送される場合（エラーを再現するためなど）に、非実稼働環境におけるセキュリティとプライバシーの保護が実稼働環境のものと同等であることを確認します。

4.3　　サプライヤーは、転送中および保管中のキンドリル資料を暗号化します（サプライヤーが、保管中のキンドリル資料の暗号化が技術的に不可能であるとキンドリルが合理的に満足するように立証できる場合はこの限りではありません）。サプライヤーは、バックアップ・ファイルを含む媒体など、物理的な記憶媒体がある場合もすべて暗号化します。サプライヤーは、安全な鍵の生成、発行、配布、保管、ローテーション、失効、回復、バックアップ、破棄、アクセス、およびデータ暗号化に関連した使用に関する文書化された手順を実施します。サプライヤーは、そのような暗号化に使用される特定の暗号化方法が業界のベスト・プラクティス（NIST SP 800-131a など）に準拠していることを確認します。

4.4　　サプライヤーがキンドリル資料にアクセスする必要がある場合、サプライヤーはそのアクセスを、サービスおよび成果物を提供およびサポートするために必要な最小限のレベルに制限します。サプライヤーは、基礎となるコンポーネントへの管理アクセス（特権アクセス）を含むそのようなアクセスは、個人の役割に基づいており、職務の分離の原則に従って、許可されたサプライヤーの従業員が承認と定期的な検証の対象となるようにします。サプライヤーは、重複したアカウントや休眠アカウントを特定して削除するための措置を実施します。サプライヤーはまた、アカウント所有者の離職後、またはキンドリルもしくはアカウント所有者のマネージャーなど、承認されたサプライヤーの従業員が要求する場合、24 時間以内に特権アクセスを持つアカウントを取り消します。

4.5　　サプライヤーは、業界のベスト・プラクティスに従った技術的な対策を実施し、非アクティブなセッションのタイムアウト、ログイン試行に連続して複数回失敗した後のアカウントのロック

アウト、強力なパスワードとパスフレーズの認証、およびそのようなパスワードとパスフレーズの安全な転送と保管を要求する手段を義務付けます。さらに、サプライヤーは、キンドリル資料へのすべての非コンソールベースの特権アクセスに多要素認証を利用します。

4.6　サプライヤーは、(a) 不正なアクセスと活動を特定するため、(b) そのようなアクセスおよび活動に対し、適時かつ適切に対応しやすくするため、(c) （本規約におけるその検証する権利、および取引文書、関連する基本契約、または当事者間のその他の関連契約における監査権によって）サプライヤーがキンドリルまたはその他が、文書化されたサプライヤーのポリシーを遵守していることを監査するため、特権アクセスの使用を監視し、セキュリティ情報とイベント管理措置を実施します。

4.7　サプライヤーは、業界のベスト・プラクティスに従って、サービスまたは成果物の提供とキンドリルのテクノロジーの取り扱いにおいて使用されるシステムへの、またはシステムに関するすべての管理、ユーザー、またははその他のアクセスやアクティビティーを記録するログを保持します（要求された場合は、それらのログをキンドリルに提供します）。サプライヤーは、そのログを不正アクセス、変更、偶発的または意図的な破壊から保護することを目的とする措置を実施します。

4.8　サプライヤーは、自身が所有または管理し、サービスまたは成果物の提供またはキンドリルのテクノロジーの取り扱いに使用するシステム（エンド・ユーザーのシステムを含む）のコンピューティングの保護を確保します。これらの保護手段には、エンドポイントのファイアウォール、ディスク全体の暗号化、マルウェアの脅威や高度で持続的な脅威に対処するための署名と非署名に基づくをエンドポイント検出および応答テクノロジー、時間ベースの画面ロック、セキュリティ構成とパッチ要件を適用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。さらに、サプライヤーは、既知の信頼できるエンド・ユーザー・システムのみがサプライヤー・ネットワークの使用を許可されるように、技術的および運用上の管理を実装します。

4.9　サプライヤーは、業界のベスト・プラクティスに従い、キンドリル資料が存在する、または処理されるデータセンター環境を侵入の検出と防止や DoS 攻撃の対策と軽減などによって保護します。

5.　サービスとシステムの完全性と可用性の管理

5.1　サプライヤーは、以下を行います。(a) セキュリティ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回実施する。(b) 製品リリースの前およびリリース以降は、サービスと成果物に関して毎年、キリンドルのテクノロジーの取り扱いに関しては毎年、セキュリティ・テストを実施し、脆弱性を評価する（自動化システムとアプリケーションのセキュリティ・スキャンと手作業による倫理的ハッキングを含む）。(c) 適格な独立した第三者に、業界のベスト・プラクティスに沿ったペネトレーション・テスト（自動化されたテストおよび手動のテストの両方を含む）を少なくとも年に 1 回実施することを依頼する。(d) サービスと成果物の各コンポーネントとキンドリルのテクノロジーの取り扱いに関するセキュリティ構成要件の遵守について、自動化管理とルーチン検証を実施する。(e) 関連するリスク、悪用可能性、影響に基づいて、特定された脆弱性またはセキュリティ構成要件の違反を修正する。 サプライヤーは、テスト、評価、スキャン、および修復活動の実行時に、サービスの中断を回避するための合理的な措置を講じます。キンドリルが要求する場合、サプライヤーは、その時点で最新のサプライヤーの侵入テスト業務の要約を書面でキンドリルに提供します。この報告には、少なくとも、テストの対象となる製品の名前、テストの対象となるシステムまたはアプリケーションの数、テストの実施日、テストで使用された方法論、および調査結果の概要が含まれます。

5.2　サプライヤーは、サービスまたは成果物への変更の適用、またはキンドリルのテクノロジーの取り扱いに関連するリスクを管理することを目的とするポリシーと手順を実施します。サプライヤーは、影響を受けるシステム、ネットワーク、および基盤となるコンポーネントを含め、変更を実装する前に、登録済みの変更要求の中で(a) 変更の説明と理由、(b) 実装の詳細とスケジュール、

(c) サービスおよび成果物、サービスの顧客、またはキンドリル資料への影響に対処するリスクステートメント、(d) 予想される結果、(e) ロールバック計画、および (f) 承認されたサプライヤーの従業員による承認を文書化します。

5.3　サプライヤーは、サービスの運用、成果物の提供、キンドリルのテクノロジーの取り扱いに使用するすべての IT 資産のインベントリーを維持します。サプライヤーは、資産、サービス、成果物、キンドリルのテクノロジーの基盤となるコンポーネントなどを対象として、IT 資産、サービス、成果物、キンドリルのテクノロジーの健全性（キャパシティーを含む）と可用性を継続的に監視および管理します。

5.4　サプライヤーは、サービスおよび成果物の開発または運用、およびキンドリルのテクノロジーの取り扱いにおいて使用するすべてのシステムを、Center for Internet Security（CIS）のベンチマークなどの業界のベスト・プラクティスを満たす、定義済みのシステム・セキュリティ・イメージまたはセキュリティ・ベースラインから構築します。

5.5　取引文書または関連する両当事者間の基本契約に基づく事業継続性に関するサプライヤーの義務またはキンドリルの権利を制限することなく、サプライヤーは、事業と IT の継続性と災害復旧の要件について、文書化されたリスク管理ガイドラインに従って、各サービスと成果物、およびキンドリルのテクノロジーの取り扱いに使用される各 IT システムを個別に評価します。サプライヤーは、そのようなサービス、成果物、および IT システムのそれぞれが、そのようなリスク評価によって正当化される範囲で、事業と IT の継続性および災害復旧計画を個別に定義、文書化、実施、毎年検証し、業界のベスト・ プラクティスと整合することを確認します。サプライヤーは、その計画が、以下の第 5 条 6 項に規定されている特定の復旧時間を実現するように設計されていることを確認します。

5.6　ホスティング・サービスに関する具体的な目標復旧時点（「**RPO**」）および目標復旧時間（「**RTO**」）は、RPO、RTO 共に 24 時間ですが、キンドリルがより短時間の RPO または RTO を書面で通知する場合（電子メールは書面とみなします）、サプライヤーはキンドリルがお客様に約束した、目標より短時間の RPO または RTO を遵守します。サプライヤーがキンドリルに提供する他のすべてのサービスに関係するため、サプライヤーは、自身の事業継続性と災害復旧計画が、適時にテスト、サポート、および保守を提供する義務を含む、取引文書および関連する両当事者間の基本契約、および本規約に基づく、サプライヤーのキンドリルに対するすべての義務を遂行し続けることを可能にする RPO および RTO を実現するように作成されていることを確認します。

5.7　サプライヤーは、サービスおよび成果物、ならびにその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、ならびにキンドリルの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、テストし、それらにセキュリティ・アドバイザリー・パッチを適用するために設計された措置を実施します。セキュリティ・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する場合、サプライヤーは文書化された重大度およびリスク評価ガイドラインに従ってパッチを実装します。サプライヤーによるセキュリティ・アドバイザリー・パッチの実装は、その変更管理ポリシーの対象となります。

5.8　サプライヤーがキンドリル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キンドリルが判断する合理的な根拠がある場合、サプライヤーは、キンドリルの懸念事項の調査および修復において、キンドリルに適時に協力します。

6.　サービスのプロビジョニング

6.1　サプライヤーは、キンドリル・ユーザーまたはお客様のアカウントのフェデレーション方式の認証についての業界共通の方法をサポートし、サプライヤーはこのキンドリル・ユーザーまたはお客様のアカウントを認証する際、業界のベスト・プラクティスに従います（キンドリルによる

OpenID Connect または Security Assertion Markup Language を使用した、一元管理された多要素シングルサインオンなど）。

7. **「復処理者」**。取引文書または両当事者間の関連する基本契約に基づく、従契約者の維持に関するサプライヤーの義務またはキンドリルの権利を制限することなく、サプライヤーは、サプライヤーのために作業を遂行する従契約者が、本規約がサプライヤーに課す要件および義務を遵守するためのガバナンス管理を確立していることを確認します。

8. **「物理メディア」**。サプライヤーは、再利用を目的とした物理的な記憶媒体を安全に殺菌してから再利用し、再利用を目的としていない物理的な記憶媒体を破棄し、媒体の殺菌に関する業界のベスト・プラクティスに従います。

第9条　ホスティング・サービスの証明書および報告書

本条項は、サプライヤーがキンドリルにホスティング・サービスを提供する場合に適用されます。

1.1　　サプライヤーは、以下に定める期間内に、次の証明書または報告書を取得します。

証明書/報告書	**期日**
サプライヤーのホスティング・サービスに関して： 国際標準化機構（ISO）27001、有名な独立監査法人による査定に基づく情報技術、セキュリティ技術、情報セキュリティ管理システムの遵守に関する認証。 **または** SOC 2 Type 2：SOC 2 Type 2に従って（少なくともセキュリティ、機密性および可用性を含む）、評価の高い独立監査人が実施した、サプライヤーのシステム、制御および運用のレビューを立証する報告書	サプライヤーは、取引文書*の発効日または想定日**から120日後までにISO 27001認証を取得し、その後12か月ごとに、有名な独立監査法人の評価に基づいて認証を更新します（その時点で標準の最新バージョンに準じて更新）。 サプライヤーは、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、SOC 2 Type 2に従って、評判の高い独立監査人が実施する、サプライヤーのシステム、制御および運用のレビューを立証する、新規報告書（少なくともセキュリティ、機密性および可用性を含む）を12か月ごとに取得します。 * その発効日の時点で、サプライヤーがホスティング・サービスを提供する場合 ** サプライヤーがホスティング・サービスを提供する義務を負う日

1.2　　サプライヤーが書面で要求し、キンドリルが書面で承認する場合、サプライヤーは、実質的に同等の証明書または報告書に関して、上記の表に記載されている期間が変更なく適用されることを理解した上で、上記の証明書または報告書と実質的に同等の証明書または報告書を取得することができます。

1.3　　サプライヤーは、(a) 要求された場合、サプライヤーが取得義務を負う各証明書および報告書の写しをキンドリルに速やかに提供し、(b) SOC 2または実質的に同等のレビュー（キンドリルがそれを承認する場合）で指摘された内部統制の脆弱性を速やかに解決します。

第10条　協力、検証および修復

本条は、サプライヤーがキンドリルにサービスまたは成果物を提供する場合に適用されます。

1.　　サプライヤーの協力

1.1　　サービスまたは成果物がサイバー・セキュリティ上の懸念に寄与したか、寄与しているか、または今後寄与するかについて、キンドリルが疑問を抱く理由がある場合、サプライヤーは、この懸念事項に関するキンドリルからの問い合わせに合理的に協力するものとします。こうした協力には、情報の要求（文書その他の記録、関連するサプライヤーの担当者との面談、またはこれらに類似するもの）に対する適時かつ十分な対応などが含まれます。

1.2　　両当事者は、(a) 要求された場合、追加情報を相互に提供すること、(b) それに関す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に同意します。これらはすべて、本規約と本規約において参照される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場合があります。例えば、キンドリルが要求する場合、サプライヤーがその権利を有する場合に、契約書自体へのアクセスを付与するなどによって、サプライヤーは復処理者および従契約者との書面による契約のプライバシーとセキュリティに焦点を当てた条項を適時に規定します。

1.3　　キンドリルが要求する場合、サプライヤーは、その成果物およびそれらの成果物のコンポーネントが製造、開発、またはその他の方法で調達された国に関する情報を適時に提供します。

2.　　検証（以下で使用される「施設」とは、サプライヤーがキンドリル資料をホスティング、処理、またはその他の方法でアクセスする物理的な場所を意味します）

2.1　　サプライヤーは、本規約の遵守を示す監査可能な記録を保持します。

2.2　　キンドリルは、単独で、または外部監査人とともに、サプライヤーに 30 日前までに書面で通知することにより、サプライヤーによる本規約の遵守を確認することができます（この目的のために施設にアクセスすることを含みます）。ただし、キンドリルは、そうすることで関連情報が提供されると信じる誠実な理由がある場合を除き、サプライヤーがキンドリルのデータを処理するデータセンターにアクセスすることはありません。サプライヤーは、文書、その他の記録、関連するサプライヤー担当者の面談などを通じて、情報の要求に対する適時かつ完全な対応を含め、キンドリルの検証に協力します。サプライヤーは、キンドリルが検討するために、承認された行動規範または業界の証明書に準拠しているという証左を提供するか、または本規約の遵守を立証する情報を提供することができます。

2.3　　検証は、12 か月間に 2 回を超えて行われることはありません。ただし、(a) 12 か月間に過去の検証に起因する懸念に対するサプライヤーの是正をキンドリルが確認している場合、または (b) セキュリティ侵害が発生し、キンドリルが侵害に関連した義務の履行の検証を希望している場合を除きます。いずれの場合も、キンドリルは上記の第 2 条 2 項で指定されているのと同様に、30 日前までに書面により通知しますが、セキュリティ侵害に対処する緊急性により、キンドリルは 30 日より短い期間で書面で通知して検証する必要がある場合があります。

2.4.　　規制当局またはその他の管理者は、規制当局が法の下で有する追加の権利を行使できることを理解した上で、第 2 条 2 項および第 2 条 3 項でキンドリルと同じ権利を行使することができます。

2.5　　キンドリルに、サプライヤーがこれらの条件のいずれかを遵守していないと結論付ける合理的な根拠がある場合（そのような根拠が、本規約に基づく検証またはその他に起因するかにかかわらず）、サプライヤーはそのような不履行を速やかに是正します。

3.　　偽造防止プログラム

3.1　　サプライヤーの成果物に電子部品（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、中央処理装置、論理デバイスまたはケーブルなど）が含まれる場合、サプライヤーは、文書化された偽造防止プログラムを実施し、これに従います。まず第一に、サプライヤーが偽造コンポーネントをキンドリルに供給することを防止し、次に、サプライヤーが偽造コンポーネントをキンドリルに誤って提供した場合には、速やかに検出して修復します。 サプライヤーは、キンドリルに対するサプライヤーの成果物に含まれる電子部品を提供するすべてのサプライヤーに対して、文書化された偽造防止プログラムを実施し、これに従うという同じ義務を課すものとします。

4.　　修復

4.1　　サプライヤーが本規約に基づく義務のいずれかを遵守できず、その不履行がセキュリティ侵害の原因となった場合、サプライヤーは、キンドリルの合理的な指示とスケジュールに従って、履行と修復を行うことで、その不履行を修正し、セキュリティ侵害の悪影響を修復します。 ただし、サプライヤーによるマルチテナントのホスティング・サービスの提供に起因してセキュリティ侵害が発生し、その結果、キンドリルを含む多くのサプライヤーのお客様に影響を与える場合、サプライヤーは、セキュリティ侵害の性質を考慮して、機能不全を適時かつ適切に修正し、セキュリティ侵害の有害な影響を修復する一方で、そのような修正と修復に関するキンドリルの意見を十分に考慮します。 上記を損なうことなく、適用されるデータ保護法によって設定された義務をサプライヤーが遵守できなくなった場合、サプライヤーは遅滞なくキンドリルに通知する必要があります。

4.2　　キンドリルは、そうすることが適切または必要と思われる場合には、第 4 条 1 項で言及されているセキュリティ侵害の修復に参加する権利を有し、その際、サプライヤーは、その履行を修正する際の費用および経費、およびそのようなセキュリティ侵害に関して両当事者が負担する修復費用と経費に対して責任を負います。

4.3　　例えば、セキュリティ侵害に関連する修正費用および経費には、セキュリティ侵害の検出と調査、適用される法律および規制に基づく責任範囲の決定、侵害の通知の提供、コール・センターの設立と維持、信用監視および信用回復サービスの提供、データのリロード、製品の欠陥の修正（ソース・コードまたはその他の開発によるものを含む）、上記またはその他の関連する活動を支援する第三者の確保、セキュリティ侵害の悪影響を是正するために必要なその他の費用および経費などが含まれる可能性があります。明確にすると、修正費用および経費には、キンドリルの逸失利益、事業価値、収益、信用、または予想される節減の喪失は含まれていません。