サプライヤーのプライバシーおよびセキュリティに関する規約

この「サプライヤーのプライバシーおよびセキュリティに関する規約」（以下、「**本規約**」）は、データ・ガバナンス、セキュリティおよび関連する事項に関するキンドリルおよびサプライヤーの権利および義務を定めるものです。本規約は、両当事者間の Supplier Relationship Agreement もしくは同等の契約（SOW、WA を含む）、または当該契約に言及する両当事者間の他の文書（以下、「**取引文書**」）に組み込まれ、その一部を構成します。

本規約は、以下で構成されます。

- この文書
- この文書に添付される「処理の詳細に関する別紙」。これは、本規約の締結時点におけるサプライヤーのデータ処理業務についての概要を記載したものです（本規約の締結後に作成される各取引文書には、当該取引文書に固有のサプライヤーの処理活動を記載した、別個の「処理の詳細に関する別紙」が添付されます）。
- EU 標準契約条項、英国国際データ転送補遺およびサプライヤー移転影響評価（https://www.kyndryl.com/procurement/terms/privacy-and-security-terms でご覧いただけます）。

本規約、Supplier Relationship Agreement、同等の契約または取引文書（データ処理契約を含む）の規定の間に矛盾がある場合、本規約を優先します。本規約と、キンドリルのお客様に関してサプライヤーとキンドリル間で合意した規定との間に矛盾がある場合には、キンドリルのお客様に関して合意した条件を優先します。

定義語（英語版において大文字で始まる語）は、本規約の第 5 条、本規約内のそれ以外の箇所、または取引文書もしくは両当事者間の関連する基本契約に定める意味を有します。

第 *1* 条　データ・ガバナンスおよび AI

1.1. **法令遵守。**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法律（データ保護、サイバー・セキュリティおよび AI システムに関する法律を含む）を遵守します。サプライヤーは、自己の法的義務をもはや果たすことができないと判断した場合には、速やかに（いかなる場合も、法律により義務付けられており、キンドリルがキンドリル自身の法的義務を履行する機会を与えられる時間枠内に）キンドリルに通知します。

1.2. **データの使用。**サプライヤーは、以下のことを行いません。

(a) サービスおよび成果物を提供する以外の目的で、集約化、匿名化その他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（例えば、サプライヤーは、サービスや成果物以外の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作成を目的として、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ません）。

(b) キンドリルのデータを販売または共有すること。

(c) データ主体に関する情報を推測するため、またはその他の方法でデータ主体に結び付けるために合理的に使用することが可能な情報について、再特定化を試みること。

1.3. **Web追跡技術。**サプライヤーまたはその従契約者が、サービスまたは成果物の引渡しにおいて、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ビーコンを含む）を使用してデータを収集する場合、当該データは、キンドリルのデータとみなされ、サプライヤーは、本規約に基づきキンドリルのデータに関する自らの義務を遵守します。

1.4. **非開示。**サプライヤーは、第2.5条に従って承認された復処理者や本契約に従って承認された従契約者以外の第三者に対して、キンドリルのデータを開示しないものとします。

1.5. **政府によるアクセス。**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（米国政府がキンドリルのデータを取得するためにサプライヤーに対して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る場合、サプライヤーは、法律で禁止されていない限り、キンドリルにその請求または要求を書面で速やかに通知し、キンドリルが開示に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。通知が法律によって禁止されているときには、サプライヤーは、裁判その他の手段を通じて、当該禁止またはキンドリルのデータの開示に異議を唱えるために適切であるとサプライヤーが合理的に判断する措置を講じます。

1.6. **機密保持。**サプライヤーは、キンドリルに対して以下のとおり保証します。(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のあるサプライヤーの従業員のみが、必要な範囲に限って、当該アクセスを有すること、ならびに (b) サプライヤーの従業員に機密保持義務を課し、本規約により許容され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ていること。

1.7. **キンドリルのデータの返却または削除**。取引文書の解約もしくは期間満了時に、またはそれより前にキンドリルが要求した時に、サプライヤーは、自己の費用負担で、キンドリルの選択に従い、キンドリルのデータを削除し、またはキンドリルに返却します。キンドリルが削除を要求した場合、サプライヤーは、NIST SP 800-88 rev.1に従って、データを読み取り不能にし、再構築や復元ができないようにしたうえで、キンドリルの要請に応じてこれを削除したこと証明します。キンドリルが、キンドリルのデータの返却を要求した場合、サプライヤーは、キンドリルの合理的なスケジュールおよび指示に従って、一般に使用されるフォーマットにより返却します。

1.8. **AIシステム**

(a) 取引文書または本契約においてキンドリルの事前許可がない限り、サプライヤーは、サービスもしくは成果物の引渡しにおいて AI システムを使用してはならず、成果物に AI システムを含めてもなりません。キンドリルの許可を求める際、サプライヤーは、サプライヤーによる AI システムの使用を評価するために必要なすべての情報（データ・フロー、使用される言語モデル、データ分離など）を、キンドリルに書面で提供します。

(b) サプライヤーは、以下のことを表明および保証します。(i) キンドリルから提供されたインプット（取引文書に基づき従業員その他第三者から提供されたインプットを含む）およびアウトプットが、キンドリル資料に分類されること、(ii) サプライヤーが、キンドリル資料を使用して、基盤モデルまたは AI システムの他の要素のトレーニングまたはファインチューニングを行わないこと、(iii) サプライヤーが、サービスの提供に必要な期間を超えてキンドリル資料を保存しないこと、(iv) AI システム（アウトプットおよびトレーニング・データを含む）が、サービスの一部に分類されること、ならびに (v) 適用法により許容される範囲で、サプライヤーが本書により、AI システムのアウトプットに係る自らの権利、権原および権益のすべてをキンドリルに譲渡すること。

(c) サプライヤーは、AI システムに関して、AI システムに関連または起因する既知および予測可能なリスク（倫理、バイアス、セキュリティおよび安全性に関するリスクを含むが、これらに限らない）を特定し、テストし、監視し、合理的かつ適切に軽減する、文書化されたガバナンスおよびリスク管理プログラムを導入し、維持するものとします。サプライヤーは、要請に応じて、AI システムに関する自らのガバナンスおよびリスク管理プログラムのコピーを共有します。サプライヤーは、発生したリスクまたは特定された重大なリスクについて、取引文書において合意された通知規定に従って、速やかに書面でキンドリルに通知します（コピーを ailegalteam@kyndryl.com に送信します）。

第 *2* 条　プライバシー

2.1. **連絡先個人情報**。キンドリルおよびサプライヤーは、成果物およびサービスの引渡しおよび受領に伴う業務を行う場合は常に、独立した管理者として、適用されるデータ保護法に従って相手方の BCI を処理することができます。両当事者は、相手方の BCI に関して共同管理者として行動するものではありません。いずれかの当事者が、他方当事者の BCI に関してデータ主体から受けた要請を他方当事者に知らせた場合、他方当事者は、直接そのデータ主体と共に、当該要請に対処する責任を負います。両当事者はそれぞれ、他方当事者の BCI を保護するための適切な技術的および組織的措置を導入しています。明確にするために記すと、第 3.12 条（セキュリティ・インシデント）は、BCI に適用されます。

2.2. **処理者としてのサプライヤー**。キンドリルは、キンドリルの指示（本規約、本契約および関連する取引文書に記載された指示を含む）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たキンドリルの個人データの処理者として、サプライヤーを指名します。サプライヤーは、キンドリルの個人データの処理者です。サプライヤーが、キンドリルが適用されるデータ保護法を遵守することができるようにキンドリルから指示を受けた場合に、これに応じないときは、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することができます。サプライヤーは、指示がデータ保護法に違反すると判断した場合、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。

2.3. **技術的および組織的措置**。サプライヤーは、セキュリティのレベルを、サービスおよび成果物の引渡しに関連するリスクに適したレベルにするために、適切な技術的および組織的措置（下記第 3 条のセキュリティ措置を含む）を導入し、維持します。

2.4. **データ主体の権利と要求**

a) 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、そのような要請を行ったデータ主体を、キンドリルに速やかに差し向けることもできます。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。

b) 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。

2.5. **復処理者**

a) キンドリルは、サプライヤーが、各「処理の詳細に関する別紙」に記載された復処理者に委託することを許可します。キンドリルはさらに、サプライヤーが、以下の条件に従って、追加もしくは後継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を許可します。

(i) サプライヤーは、新規の復処理者を追加し、もしくは既存の復処理者を交替させ、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、キンドリルに書面で事前に通知します。

(ii) キンドリルは、前記の新規もしくは後継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。

(iii) キンドリルがサプライヤーの書面通知を受領してから 30 日以内に異議を提起していなければ、サプライヤーは、新規もしくは後継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。

b) サプライヤーは、復処理者がキンドリルの個人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、本規約に定めるデータ保護、セキュリティ、証明の義務を課します。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。

2.6. **域外でのデータ処理**

a) サプライヤーは、第 2.5 条に従って承認された復処理者に対する場合を除き、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を含め）転送も開示もしないものとします。キンドリルがキンドリルの個人データの越境転送を承認した場合、両当事者は、協力して適用されるデータ保護法を遵守します。これらの法律で標準契約条項（SCC）が求められる場合、サプライヤーは、下記の定めに従い、速やかに SCC を締結します。

b) **欧州経済領域**

(i) キンドリルが、EU一般データ保護規則（2016/679）(以下、GDPR)の対象となる個人データを、欧州経済領域から十分性認定国で設立されていないサプライヤーに転送する場合、サプライヤーは、キンドリルによって事前署名されたEU標準契約条項（委員会決定2021/914）（https://www.kyndryl.com/procurement/terms/privacy-and-security-terms で閲覧可能。以下、「**EU SCC**」）を、ここに締結します。

(ii) キンドリルが事実上消滅し、法律上存在しなくなり、または支払不能となった場合には、その他の管理者は、本契約を解約し、キンドリルの個人データを消去または返却するようサプライヤーに指示することができます。

(iii) EU SCCによって義務付けられているとおり、サプライヤーに対する個人データ転送に関してキンドリルが行った評価は、サプライヤーの閲覧に供するために、https://www.kyndryl.com/ procurement/terms/privacy-and-security-termsで公表されています。

(iv) サプライヤーは、EU標準契約条項の第14条(c)に基づくデータ輸入者としての自己の義務を果たすために、「処理の詳細に関する別紙」および通知において、各復処理者の十分な詳細情報（復処理者の名前、処理の場所および処理活動を含む）を提供します。

(v) サプライヤーは、データ輸出者として行動し、十分性認定国で設立されていない承認された各復処理者と、EU SCCその他適切な転送の取決めを締結します。

c) **英国。**英国データ保護法（2018）の対象であるキンドリルの個人データが、英国から非十分性認定国に転送される場合、サプライヤーは、キンドリルによって事前署名された英国国際データ転送補遺（[https://www.kyndryl.com/procurement/terms/privacy-and-security-terms]で閲覧可能）をここに締結します。

d) **スイス**。スイス連邦データ保護法（以下、「**FADP**」）の対象であるキンドリルの個人データが、スイスから非十分性認定国に転送される場合、サプライヤーは、以下の修正を加えたうえで、EU SCCをここに締結します。

(i) GDPR への言及には、FADP の同等規定への言及も含まれます。

(ii) スイス連邦データ保護情報コミッショナーを、EU SCC の第 13 条および付録 I.C に基づく専属監督機関とします。

(iii) データ転送にFADPのみが適用される場合には、EU SCCの第17条に基づく準拠法は、スイス法とします。

(iv) 「加盟国」という用語は、スイス内のデータ主体について、EU SCCの第18条に従って常居所（スイス）で自己の権利に関して訴訟を行う可能性を排除するように解釈してはなりません。

e) **その他の国**。キンドリルの個人データの転送が、監督機関が現地のSCCを公表していない国のデータ保護法（ブラジル・データ保護法、ペルー・データ保護法、南アフリカ・データ保護法など）、または監督機関が越境転送のための十分な保護措置としてEU標準契約条項の使用を承認した国のデータ保護法（アルゼンチン・データ保護法など）の対象となる場合、以下の修正を加えたうえで、EU SCCが当該転送に適用されるものとします。

(i) GDPR への言及には、現地のデータ保護法の同等規定への言及も含まれます。

(ii) 現地の監督機関を、EU SCC の第 13 条および付録 I.C に基づく専属監督機関とします。

(iii) EU SCCの第17条に基づく準拠法は、現地のデータ保護法とします。

(iv) 「加盟国」という用語は、当該国のデータ主体について、EU SCCの第18条に従って常居所で自己の権利に関して訴訟を行う可能性を排除するように解釈してはなりません。

2.7. 支援と記録

(a) サプライヤーは、処理の性質を考慮して、適切な技術的および組織的措置（以下、「**TOM**」）を設けることにより、キンドリルが、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際に支援します。サプライヤーはまた、自らが入手可能な情報を考慮して、キンドリルが、処理のセキュリティ、セキュリティ・インシデントの通知および連絡、ならびにデータ保護影響評価の作成に関する義務の遵守を確実にする際に支援します（必要に応じて、担当規制当局と事前に協議することを含む）。

(b) 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。

2.8. 国別必須条件

a) 日本

i) 日本に所在するデータ主体の BCI に関して、サプライヤーは、処理者としてのサプライヤーに適用される、本規約の条件を遵守します。

ii) 本規約における「セキュリティ・インシデント」の定義は、日本に所在するデータ主体に関するキンドリルの個人データについて、その合理的に疑われる侵害を含むように、ここに修正されます。

iii) サプライヤーは、サプライヤーまたはその復処理者がキンドリルの個人データを処理する国の法および慣行によって、サプライヤーによる本規約に基づく義務の履行が妨げられると信じる理由がサプライヤー側にないことを保証します。サプライヤーは、本規約に同意した後、本規約の期間中に、本規約に基づく義務を遵守することができないと信じる理由がサプライヤー側にある場合には、キンドリルに通知します。この場合、両当事者は、その状況に対処するために講じられる適切な措置を特定するために、誠実に協力します。適切な措置を実施することができない場合、キンドリルは、キンドリルの個人データの転送を中止するか否かの評価を行います。

b) **カリフォルニア**。サプライヤーが、処理者として、カリフォルニア州に所在するデータ主体に関するキンドリルの個人データを処理する場合、(i) キンドリルは、該当する「処理の詳細に関する別紙」において選択された限定的かつ特定の事業目的に限って、キンドリルの個人データをサプライヤーに開示し、(ii) キンドリルは、通知をもって、不正な処理を停止するため、またはサプライヤーによる処理が適用されるデータ保護法に基づくキンドリルの義務に沿うようにするための合理的かつ適切な措置を講じることができ、(iii) サプライヤーは、キンドリルとサプライヤー間の直接的な事業関係外で、キンドリルの個人データを保持、使用または開示しません。

第 *3* 条　一般的なセキュリティ

3.1. セキュリティ・ポリシー

a) **ポリシー。**サプライヤーの情報セキュリティ・ポリシーは、文書化され、サプライヤーの上級管理者によって承認され、かつ、業界標準慣行と一致しているものとします。サプライヤーの情報セキュリティ・ポリシーは、継続的な適用可能性および有効性を確認するために、サプライヤーによって最低でも年 1 回、およびポリシーに重大な変更が行われた場合にはその後速やかに、見直しおよび評価が行われます。サプライヤーは、キンドリル資料、成果物またはサービスに関するサプライヤーのセキュリティを低下させることになるようなポリシーの変更を行いません。

b) **テスト。**サプライヤーは、キンドリル資料、成果物およびサービスのセキュリティを確実にするための技術的および組織的措置の有効性を、定期的にテストするプロセスを維持します。

c) **リスク管理。**サプライヤーは、進行中のリスク・ガバナンス・プログラムの一環として、以下を目的とした適切な情報セキュリティ・リスク評価を実施します。(i) キンドリル資料、成果物およびサービスに関する情報セキュリティ・リスクを特定すること、(ii) 当該リスクの影響を評価すること、ならびに (iii) リスク削減または軽減戦略が特定または是認された場合には、脅威の状況が絶えず変化することを認識した上で、当該リスクを軽減し、効果的に管理する措置を導入すること。

3.2. 関係者のセキュリティ

a) **セキュリティ研修**。サプライヤーは、キンドリル資料、成果物またはサービスへのアクセスを有する、またはアクセスが可能なすべてのサプライヤーの関係者に、セキュリティおよびプライバシーに関する適切な意識啓発、教育および研修を少なくとも年 1 回行います。

b) **背景調査。**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的な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関係者およびサプライヤーが支配する子会社の関係者にも拡大適用します。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。

3.3. 資産管理

a) **資産目録**。サプライヤーは、キンドリル資料が保存されているすべての機器の資産目録を維持します。サプライヤーは、当該機器へのアクセスを、許可されたサプライヤーの関係者のみに制限します。サプライヤーは、キンドリル資料への不正なアクセス、およびキンドリル資料のコピー、修正、除去を防止します。サプライヤーは、キンドリル資料の不正なアクセス、コピー、修正または削除を防止する措置を維持します。

b) **ソフトウェア・コンポーネントのセキュリティ**。サプライヤーは、サービスの提供ならびに成果物の開発および提供に使用されるすべてのソフトウェア・コンポーネント（オープンソース・ソフトウェアを含む）を、適切に目録に記載することに同意します。サプライヤーは、当該ソフトウェア・コンポーネントが、キンドリル資料、成果物またはサービスの不正な開示やこれらへのアクセスを生じさせる可能性のある、セキュリティ上の欠陥および／または脆弱性を有するか否かを評価します。サプライヤーは、サービスおよび成果物を引き渡す前、またはこれらへのアクセスをキンドリルに認める前に、ならびにその後取引文書の期間中は継続的に、当該評価を実施します。サプライヤーは、サプライヤーが気付いた当該ソフトウェア・コンポーネントに存するセキュリティ上の欠陥または脆弱性を、適時に是正することに同意します。サプライヤーは、当該ソフトウェア・コンポーネントに存するセキュリティ上の欠陥もしくは脆弱性をサプライヤーが把握しているか否か、および／またはそれらをサプライヤーが是正したか否かに関するキンドリルからの問合せに、速やかに応答します。

3.4. アクセス制御ポリシー。サプライヤーは、キンドリル資料へのアクセスおよびサービス提供のために使用されるサプライヤーの資産へのアクセスを、許可されたサプライヤーの関係者のみに制限するため、ならびに当該アクセスを、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するために、業界標準慣行に沿った適切なロールベース・アクセス制御ポリシーおよび適切なアクセス制御技術措置を維持します。

3.5. 権限付与

a) サプライヤーは、すべてのキンドリル資料ならびにサービスおよび成果物の提供において使用されるすべてのサプライヤーの内部アプリケーションおよび資産へのアクセスを許可するため、および速やかに（いかなる場合も 24 時間以内に）取り消すために、ユーザー・アカウントの作成および削除手順を維持します。サプライヤーは、ユーザー・アカウントの作成および取消し、または既存アカウントのアクセス・レベルの引上げもしくは引下げ（関係者の雇用、契約、委託その他サプライヤーとの合意の終了のほか、当該関係者が当該アクセス権をもはや必要としなくなった場合の役割の変更を含む）を承認する適切な権限を割り当てます。

b) サプライヤーは、システムおよび資産のうち、キンドリル資料および成果物が保存されているもの、これらにアクセスすることができるもの、またはサービスの提供に使用されるものへのアクセスを許可されたサプライヤーの関係者の記録を維持および更新し、当該記録を少なくとも四半期ごとに見直します。管理および技術サポート関係者は、要求された場合に限り、かつ、当該関係者が適用されるサプライヤーの技術的および組織的措置を遵守することを条件として、当該システム、キンドリル資料および成果物にアクセスを有することを認められます。

c) サプライヤーは、当該システムおよび資産にアクセスすることができるユーザー・アカウントが、一意的なものであり、パスワードによって制限されていること、ならびにユーザー・アカウントが共有されないことを確実にします。

3.6. 認証

a) サプライヤーは、情報システムおよび資産への繰り返されるアクセスの試みを監視します。

b) サプライヤーは、形式を問わず生成され、割り当てられ、配布され、保存されるパスワードの機密保持および完全性を維持するために、業界標準慣行に沿ったパスワード保護慣行を維持します。サプライヤーは、無作為に生成された強力で複雑なパスワードもしくはパスフレーズまたは適切

な代替物（デジタル証明書、カード／ハードウェア・トークン、生体認証など）を生成し、または作成および使用するようユーザーに要求します。

c) サプライヤーは、ドメインおよびクラウド・ポータル管理アクセスなどについて、多要素認証を使用します。多要素認証には、暗号化証明書、ワンタイムパスワード（OTP）トークン、生体認証の使用などの手法が含まれます。

3.7. 暗号手法

a) **ポリシー**。サプライヤーは、該当する場合には仮名化および暗号化などにより、キンドリル資料を保護するために、業界標準慣行に沿った暗号化ポリシーおよび基準を導入し、維持します。

b) **暗号化**。サプライヤーは、転送中および保存中のキンドリル資料を暗号化するものとします。暗号化アルゴリズムは、業界標準慣行に沿ったセキュリティ・レベル（NIST SP 800-131a など）でデータを保護し、業界で認められたハッシュ関数を利用します。これは、少なくとも、保存中は 256 ビット先進暗号化標準暗号化 (AES 256)、転送中は TLS v1.2 と同程度の保護を提供するものです。サプライヤーは、業界標準慣行に沿って、暗号化鍵要件、セキュリティ、ローテーションおよびライフサイクル（生成、配布、失効、アーカイブおよび廃棄を含む）を定義する鍵管理ポリシーおよび慣行を維持し、これらに従います。

3.8. 物理的および環境的セキュリティ

a) **施設へのアクセス**。サプライヤーは、施設へのアクセス許可を、自らの権限を有する関係者に制限します。

b) **中断からの保護**。サプライヤーは、合理的な努力をもって、サポート・ユーティリティの不具合によって引き起こされる停電その他中断から当該システムおよび資産を保護します。

c) **機器のセキュアな廃棄または再使用**。サプライヤーは、記憶媒体を搭載した機器の廃棄または再使用の前に、業界標準慣行に沿ったプロセスを使用して、当該機器からすべてのキンドリル資料をセキュアに削除しまたは上書きしておくものとします。

3.9. 運用上のセキュリティ

a) **運用ポリシー**。サプライヤーは、適切な運用手順およびセキュリティ運用手順を維持し、当該手順を、それらを必要とするすべての関係者の閲覧に供します。

b) **マルウェアからの保護**。サプライヤーは、当該システムおよび資産を悪意のソフトウェア（公衆ネットワークから生じる悪意のソフトウェアを含む）から保護するアンチマルウェア制御を維持するために、アンチウイルスおよびエンド・ポイント管理ソリューションを配備します。

c) **構成管理**。サプライヤーは、関係者によるソフトウェアおよびユーティリティのインストールに適用されるポリシーを整備します。

d) **変更管理**。サプライヤーは、承認されたセキュアなバージョンのコード、構成、システムおよびアプリケーションのみが実稼働環境に配備されることを確実にする手順を導入し、維持します。

e) **論理的分離**。サプライヤーは、その実稼働環境、非実稼働環境その他の環境の適切な分離を維持し、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および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実にします。

3.10. 通信のセキュリティ

a) **情報の転送**。サプライヤーは、暗号化を用いることで、施設から物理的に転送される媒体に保存されているキンドリル資料へのアクセスを制限します。サプライヤーは、データ通信機器を用いてキンドリル資料が転送されたもしくは利用に供された範囲、またはその可能性のある範囲を、確認および立証することができるようにします。

b) **ネットワーク・サービスのセキュリティ**。サプライヤーは、すべてのネットワーク・サービスおよびコンポーネントについて、当該サービスが社内で提供されるか外部に委託されるかを問わず、業界標準慣行に沿ったセキュリティ制御および手順が実施されるようにします。
c) **侵入検知**。サプライヤーは、サービスおよび成果物の提供に使用される全てのシステムについて、サービス妨害および拒否攻撃を防ぐため、侵入検知または侵入防止のシステムおよび対策を配備します。これには、セキュリティ・イベントが特定された場合にそれを阻止し、それらに対応するための継続的な監視、ならびに新リリースの発売後可能な限り速やかにシグネチャー・データベースを更新することが含まれます。
d) **ファイアウォール**。サプライヤーは、文書化され、承認されたポートおよびサービスのみを使用可能にするファイアウォールを実装します。その他すべてのポートは、「すべて拒否」モードとします。
e) **監視**。サプライヤーは、 (i) 不正なアクセスと活動を特定するため、(ii) そのようなアクセスおよび活動に対する適時かつ適切な対応を容易にするため、(iii) サプライヤーおよびキンドリルによる監査を可能にするため、特権アクセスの使用を監視し、セキュリティ情報およびイベント管理措置を維持します。
f) **ロギング**。サプライヤーは、以下で言及するセキュリティ監査を可能にするために、すべてのシステム（ファイアウォール、ルーター、ネットワーク・スイッチおよびオペレーティング・システムを含む）が、そのそれぞれのシステム・ログ施設または集中ロギング・システムにおいて情報を確実に記録するための手順を配備するものとします。サプライヤーは、(i) ログを少なくとも 180 日間保持し、(ii) ログに機密情報が含まれないようにし、(iii) 不正な修正または消去からログを保護し、(iv) 毎日ログをバックアップし、(v) ログにリスクおよび機能的異常がないかを監視するものとします。サプライヤーは、当該ログを、要請に応じてキンドリルに提供します。

3.11. システムの取得、開発およびメンテナンス

a) **アプリケーション・ハードニング**
   i) サプライヤーは、SANS Top 25 セキュリティ開発技術や OWASP Top Ten プロジェクトなどの業界標準慣行に沿った、セキュアなアプリケーション開発ポリシー、手順および基準を導入し、維持します。
   ii) セキュアなアプリケーションの設計、開発、構成、テストおよび配備を担当するサプライヤーの関係者はすべて、サービス実施および成果物に関する資格を与えられ、サプライヤーのセキュアなアプリケーション開発慣行に関する適切な研修を受けます。
b) **システム・ハードニング**
   i) サプライヤーは、オペレーティング・システムの標準的なセキュアな構成を確立し、その使用を確実にします。イメージは、基盤となるオペレーティング・システムの強化されたバージョン、およびシステムにインストールされたアプリケーションを表示するものとします。ハードニングには、不必要なアカウント（サービス・アカウントを含む）の消去、不必要なサービスの無効化または消去、パッチの適用、開いている未使用のネットワーク・ポートの閉鎖、ならびに侵入検知システムおよび／または侵入防止システムの実装が含まれます。これらのイメージは、そのセキュリティ構成を適宜更新するために、定期的に検証されるものとします。サプライヤーは、アプリケーションとオペレーティング・システム・ソフトウェアの両方に対して、パッチ・ツールおよびプロセスを実装します。旧式のシステムに、もはやパッチを適用することができない場合には、サプライヤーは、最新バージョンのアプリケーション・ソフトウェアに更新します。サプライヤーは、ソフトウェアのうち、旧版のもの、サポート対象外となったもの、および使用されていないものをシステムから消去します。
   ii) サプライヤーは、管理者権限については、オペレーティング・システムを管理するために必要な知識を有し、かつ基盤となるオペレーティング・システムの構成を修正するためにこれを業務上必要とする関係者のみに制限します。

c) **インフラストラクチャー脆弱性スキャン**。サプライヤーは、サービスおよび成果物に関係する自らの内部環境（サーバー、ネットワーク・デバイスなど）については月 1 回、サービスおよび成果物に関する外部環境については週 1 回、スキャンを行います。サプライヤーは、発生するリスクおよび重大度レベルに応じてスキャンの結果に対処するために、具体的な時間枠を含め、文書化された明確なプロセスを整備します。

d) **アプリケーション脆弱性評価**。サプライヤーは、新規パブリック・リリース前に、アプリケーション・セキュリティ脆弱性評価を実施します。サプライヤーは、発生するリスクに応じて評価結果に対処するために、文書化された明確なプロセスを整備します。

e) **侵入テストおよびセキュリティ評価**。サプライヤーは、年 1 回以上、反復的に、サービスおよび成果物の提供に関係するすべてのシステムに対し、包括的な侵入テストおよびセキュリティ評価を実施します。さらに、サプライヤーは、業界で認められている独立した第三者に、年 1 回のテストを委託します。サプライヤーは、発生するリスクに応じて評価結果に対処するために、文書化された明確なプロセスを整備します。キンドリルの書面による要請に応じて（ただし、年 1 回を限度として）、サプライヤーは、独立した第三者による侵入テストが完了したこと、およびサプライヤーがリスク評価に従って評価結果に対処するためのプロセスを導入したことを示す証明書を提出します。サプライヤーは、テストされたシステムまたはアプリケーションの数、テスト実施日、テスト方法、ならびに「重大」、「高」、「中」および「低」判定の件数を含め、評価結果の概要を提出します。

f) **災害復旧**。本契約の期間中、サプライヤーは、サービスおよび成果物について、業界標準慣行に沿った災害復旧（以下、「**DR**」）または高可用性（以下、「**HA**」）ソリューションおよび関係する計画を維持します。サプライヤーは、DR または HA ソリューションおよび関係する計画を、少なくとも年 1 回テストします。さらに、ソリューションおよび関係する計画により、以下のことを確実にするものとします。

   i) サービスおよび成果物を提供するため使用されるインストール済みのシステムに中断が生じた場合の復旧

   ii) 物理的または技術的なインシデントが生じた場合に、サプライヤーが、キンドリル資料の可用性およびこれへのアクセスを適時に復旧する能力

   iii) サプライヤーがサービスおよび成果物を提供するために使用するシステムの、継続的な機密保持、完全性、可用性および回復力

3.12. セキュリティ・インシデント

a) サプライヤーは、業界標準慣行に沿った情報セキュリティ・インシデント対応プログラムを維持し、これに従います。これには、情報セキュリティ・インシデントを調査し、これに対処するための文書化された手順が含まれます。情報セキュリティ・インシデント対応プログラムは、インシデントの優先順位付け、役割と責任、内部エスカレーション手順、追跡と報告、封じ込めと是正などのトピックに対処するものとします。情報セキュリティ・インシデント管理プログラムに対し、定期的に（ただし、少なくとも年 1 回）、テスト、見直しおよび承認を行います。

b) サプライヤーは、セキュリティ・インシデントに気付いた場合、cyber.incidents@kyndryl.com宛に電子メールを送信することにより、キンドリルに対して速やかに（いかなる場合も 48 時間以内に）通知します。セキュリティ・インシデントに関して、サプライヤーは、速やかに以下を行います。

   i) 当該インシデント、サプライヤーによるインシデントの調査、ならびにサプライヤーの是正および回復活動の状況に関する情報を合理的に要求された場合、これをキンドリルに提供する。合理的に要求される情報の例としては、インシデントの性質、原因および影響に関する実際の調査結果、デバイス、システム、サービス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のほか、デバイス、システムまたはアプリケーションのフォレンジック・イメージに基づく概要、その他類似の項目などが挙げられます。ただし、

これらは、インシデント、またはサプライヤーの軽減、是正および回復活動に関連する範囲に限ります。

ii) 当該インシデントについて把握している適切なサプライヤーの関係者が、キンドリルから要請された電話会議に出席するようにする。

iii) キンドリルの合理的な要請に応じて、インシデント対応、データ侵害インシデント管理、フォレンジックおよび電子情報開示に関する第三者内容領域専門家を雇う。

iv) キンドリル、キンドリルの関係会社、およびお客様（その顧客および関係会社を含む）の法的義務（規制当局、データ主体、お客様その他第三者に通知する義務を含む）を満たすための合理的な支援をキンドリルに提供する。

v) セキュリティ・インシデントの影響を適時かつ適切に軽減および是正し、将来において同様のインシデントが生じるリスクを削減するための追加的な制御およびプロセスを導入する。その際、当該軽減および是正に関するキンドリルの意見を十分に検討する。

c) サプライヤーは、セキュリティ・インシデントの調査、その対応、軽減および是正においてサプライヤーに生じたすべての費用および経費につき責任を負います。本契約における責任の制限を条件として、サプライヤーは、セキュリティ・インシデントの調査、その対応、軽減および是正に関連してキンドリル、キンドリルの関係会社およびお客様（ならびにその顧客および関係会社）に生じた自己負担費用および経費についても責任を負います。セキュリティ・インシデントの是正の費用および経費には、セキュリティ・インシデントの検知および調査、法規に基づく責任の決定、データのリロード、欠陥製品の修正（ソース・コードその他の開発により生じた場合を含む）、上記その他の関連する活動を支援する第三者への委託に関する費用、その他セキュリティ・インシデントの悪影響を是正するために必要な費用および経費が含まれます。

d) キンドリルの個人データが関係するセキュリティ・インシデントが生じた場合には、サプライヤーは、サプライヤーに生じた費用につき責任を負うほか、以下に関してキンドリルに生じた費用および経費をキンドリルに弁済します。

i) 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・インシデントの通知を提供すること。

ii) データ主体からのセキュリティ・インシデントおよびその結果に関する質問に回答するためにコール・センターを設置し、当該データ主体がセキュリティ・インシデントの通知を受けた日から 1 年間、または適用されるデータ保護法で義務付けられている場合はそれより長い期間、維持すること。キンドリルとサプライヤーは協力して、コール・センターのスタッフがキンドリルの個人データに関する問い合わせに対応する際に使用するスクリプトその他資料を作成します。

iii) 個人情報窃盗からの保護、信用モニタリングおよび信用回復サービスについて、インシデントによって影響を受けたデータ主体が当該サービスの登録を選択した場合、セキュリティ・インシデントの通知を受けた日から 2 年間、または適用法で義務付けられている場合はそれより長い期間、これを提供すること。

e) サプライヤーは、キンドリルから書面で承認されるか、または法律で義務付けられる場合を除き、第三者に対して、直接間接を問わず、キンドリルがセキュリティ・インシデントによる影響を受けたことを知らせないものとします。サプライヤーは、直接または間接的にキンドリルを特定する通知をなすよう、法的に義務付けられる場合、当該通知を第三者に配布する前に、キンドリルに書面で報告します。

f) サプライヤーはまた、本規約、またはサプライヤーのセキュリティ・ポリシー、セキュリティ手順、成果物もしくはサービスの引渡しに関する利用規約に対し、実際のまたは差し迫った違反の脅威が生じたときは、その旨をキンドリルに速やかに報告します。

3.13. サプライヤー関係

(a) **従契約者。**サプライヤーは、従契約者を使用する場合であっても、本規約の遵守に責任を負います。サプライヤーは、当該従契約者に、本規約においてサプライヤーに適用される条件に劣らず徹底したまたは厳格な条件により、キンドリル資料を保護することを契約上約束させます。サプライヤーは、各従契約者の履行について、キンドリルに対する責任を負います。

(b) **品質管理およびセキュリティ管理**。サプライヤーは、従契約者に外部委託したソフトウェア開発について、品質管理およびセキュリティ管理の監督を行います。

(c) **契約前情報**。サプライヤーは、キンドリルとの契約前交渉中に提供された、プライバシー、セキュリティおよびデータ・ガバナンスに関するすべての重要な情報が、本規約その他に従って提供されたかを問わず、重要なあらゆる点で正確であり、脱落その他によるかを問わず、誤解を生じさせるものではないことを、表明し保証します。

3.14. 検証、協力、セキュリティ遵守およびアセスメント

a) **検証** 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。

(i) 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関係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。

(ii) 検証は、12 か月間に複数回行われることはありません。ただし、(A) 12 か月間に、前回の検証で生じた懸念事項に対するサプライヤーによる是正状況をキンドリルが確認する場合、または (B) セキュリティ・インシデントが発生し、キンドリルが当該インシデントに関連する義務の遵守について検証を希望する場合を除きます。いずれの場合も、キンドリルは、上記第(i)項と同様に 30 日前までに書面で通知しますが、セキュリティ・インシデントに緊急に対処する必要性により、キンドリルが検証の際に行う事前通知の期間が、30 日を下回る場合があります。

(iii) 規制当局、その他の管理者（法的に権利を有する場合）は、規制当局が、法の下で有する追加的な権利を行使する場合があることを理解したうえで、第(ii)項および第(iii)項に定めるキンドリルの権利と同じ権利を行使することができます。

(iv) キンドリルに、サプライヤーが本規約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。

(v) 本条は、本契約の「記録保持および監査権」条項その他同様の監査条項に追加して適用されるものとします。

b) **協力**。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関係者との面談、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。

c) **セキュリティ遵守**。サプライヤーは、(i) 独立公認監査法人からの ISO 27001 の遵守証明書、(ii) SOC 2 Type 2 に従ってサプライヤーのシステム、統制および運用を審査したことを証明する独立公認監査法人の報告書（最低限、セキュリティ、可用性および機密保持に係る Trust サービス原則（セキュリティ原則は、コモン・クライテリアともいう）を記載したもの）、ならびに (iii) サービスがキンドリルの財務報告書に影響を及ぼす場合には、SOC 1 Type 2 に従ってサプライ

ヤーのシステム、統制および運用を審査したことを証明する独立公認監査法人の報告書を取得します。サプライヤーは、AICPA（米国会計士協会）、IAASB（国際監査・保証基準審議会）、米国証券取引委員会または公開企業会計監視委員会によって SSAE18 に関するガイダンスが将来発行された場合は、これを遵守します。要請に応じて、サプライヤーは速やかに、サプライヤーが取得する義務を有する各証明書および報告書の写しを、キンドリルに提出します。

d) **キンドリルのコンプライアンス評価**。キンドリルの合理的な要請に応じて（ただし、各個別のサービスまたは成果物について 12 か月間に 1 回まで）、サプライヤーは、自らによる本契約および本規約に基づくサイバー・セキュリティおよびデータ・ガバナンス義務状況の遵守を確認するための質問票に、正確かつ適時に（14 日以内）記入します（以下、「**コンプライアンス評価**」）。コンプライアンス評価の完成後に、キンドリルがサプライヤーのセキュリティおよびデータ・ガバナンス慣行および手順がサプライヤーの義務を充足するものではないと合理的に判断した場合には、サプライヤーに不備を通知します。サプライヤーは、不備があるとのキンドリルの評価に同意する場合、不当に遅れることなく、(i) リスク評価に基づきキンドリルと合意した時間枠内で、サプライヤーの費用負担で当該不備を是正し、(ii) 不備を是正したことを確認する合理的な文書および情報をキンドリルまたはその正式な授権代表者に提出します。サプライヤーが、「高」または「重大」と評価された不備を合意された時間枠内に是正しなかった場合には、キンドリルは、サプライヤーに対する通知をもって直ちに、重大な違反を理由として、該当する取引文書または本契約を解除することができます。キンドリルは、サプライヤーから書面同意を得ていない限り、キンドリル自身の監査人以外の第三者に文書を開示することはありません。サプライヤーは、不備があるというキンドリルの評価に同意しない場合は、速やかに、その理由を詳述した書面による説明書をキンドリルに提出し、キンドリルがサプライヤーの理由を受け入れないときは、両当事者は、その各自の最高プライバシー責任者、最高情報セキュリティ責任者、または同様の職務範囲および権限を有するエグゼクティブに、適時の解決を求めてエスカレーションを行います。キンドリルがサービスを利用したことによって不備が生じた場合には、サプライヤーは、キンドリルがサービスの適切な利用についてキンドリルに合理的な技術サポートを提供することで、当該不備の是正を図ります。

第 *4* 条　キンドリルのネットワークへのアクセス

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。

4.1. 総則

a) 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許可するかどうかを決定します。キンドリルが許可する場合、サプライヤーは、本条の要件を遵守するほか、アクセス権を有する従業員に本条の要件を遵守させます。

b) 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できる手段（キンドリルが提供するデバイスを通じてアクセスするか、サプライヤーが提供するデバイスを通じてアクセスするかなど）を特定します。

c) サプライヤーの従業員は、サービスを提供するためにのみ、会社システムにアクセスすることができ、キンドリルが当該アクセスを承認するデバイスのみを使用することができます。このデバイスは、キンドリルが提供するデバイス（以下、「キンドリルのデバイス」）またはサプライヤーが提供するデバイス（以下、「サプライヤーのデバイス」）の、いずれかとなります。

d) 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）。

e) 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。

f) 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、(i) サプライヤーに雇用されなくなった、または (ii) 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。
g) サプライヤーは、セキュリティ・インシデント（キンドリルのデバイスもしくはサプライヤーのデバイスの紛失、キンドリルのデバイスもしくはサプライヤーのデバイスまたはデータ、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。
h) 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、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。
i) 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、サプライヤーのいずれか特定の従業員またはすべての関係者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。
j) 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。

4.2. デバイス・ソフトウェア

a) サプライヤーは、その関係者に対し、会社システムへのアクセスをセキュアな方法で促進するためにキンドリルが必要とするソフトウェアを、キンドリルのデバイスおよびサプライヤーのデバイスに適時にインストールするよう指示します。サプライヤーもその関係者も、当該ソフトウェアの動作や、当該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。
b) サプライヤーとその関係者は、キンドリルが定めるキンドリルのデバイスおよびサプライヤーのデバイスの構成規則を遵守するほか、キンドリルが意図するとおりにソフトウェアが機能するように、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。
c) サプライヤーの関係者は、キンドリルのデバイスおよびサプライヤーのデバイスのユーザー名、パスワードなどを他者と共有することはできません。
d) キンドリルがサプライヤーの関係者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した場合、サプライヤーは、キンドリルが承認したサプライヤーの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、キンドリルが指示した後合理的な期間内に、当該オペレーティング・システムの新規バージョンまたは新たなオペレーティング・システムにアップグレードします。

4.3. キンドリルのデバイス

a) サプライヤーの従業員は、キンドリルのデバイスを使用して、他の個人や法人にサービスを提供することも、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・ツールまたはそれに相当するものにアクセスすることもできません。サプライヤーの従業員は、キンドリルのデバイスを私的な理由で使用することはできません（例えば、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私的なファイルを、キンドリルのデバイスに保存してはならず、私的な理由でキンドリルの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）。サプライヤーの従業員は、会社システムにアクセスするために使用するキンドリルのデバイスを、サプライヤーの他の従業員と共有することはできません。

b) 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、あらゆる方法で、あらゆる場所から、キンドリルが必要または適切であると考えるあらゆる手段を使用して、キンドリルのデバイスおよび会社システムを監視し、潜在的な侵入その他サイバー・セキュリティの脅威を是正する無条件の権利を有します。そのような権利の例として、キンドリルは、随時、(i) キンドリルのデバイス上でセキュリティ・テストを実施すること、(ii) キンドリルの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（キンドリルのデバイス上の電子メール・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を、監視し、技術的その他の手段で修復し、レビューすること、および (iii) キンドリルの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、キンドリルのデバイスを安全に構成する、キンドリルのデバイスに監視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、デバイスにインシデント対応措置を講じる、およびキンドリルが完全なフォレンジック・イメージを取得するためにキンドリルのデバイスへの物理的なアクセスを提供する要請、ならびに同様のおよび関連する要請が含まれる）。

c) 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、過失などによるキンドリルのデバイスの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修正を加えたり、修正の許可を与えたりしないものとします。修正とは、デバイスに対する変更であり、これには、デバイスのソフトウェア、アプリケーション、セキュリティ設計、セキュリティ構成や、物理的、機械的または電気的な設計の変更が含まれます。

d) サプライヤーは、キンドリルのデバイスがサービスを提供する必要がなくなってから 5 営業日以内に、それらすべてのデバイスを返却し、キンドリルが要請した場合には、同時に、これらの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、そのようなすべてのデータ、資料その他情報を永久に消去するための NIST 基準に従い、コピーを保持することなく破棄します。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された時と同様の状態で（通常の損耗を除く）梱包し、サプライヤーの費用で、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(d)項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当事者間の関連する契約の重大な違反とみなされます。ここで、ある契約が「関連する」とは、いずれかの会社システムにアクセスすることで当該契約に基づくサプライヤーの作業その他活動を容易にする場合であると解釈されます。

e) 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。

f) 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。

第 *5* 条　定義

「サービス」および「成果物」という用語は、Supplier Relationship Agreement もしくは同等の契約または取引文書においておそらく定義されていますが、定義されていない場合には、「**サービス**」とは、取引文書で明記されているとおり、サプライヤーがキンドリルのために実施するホスティング、コンサル

ティング、インストール、カスタマイズ、メンテナンス、サポート、人材の増強、業務、技術的その他の作業を意味し、「**成果物**」は、取引文書で特定されているとおり、サプライヤーがキンドリルに提供するソフトウェア・プログラム、プラットフォーム、アプリケーションその他製品またはアイテム、およびそのそれぞれの関連資料を意味します。

5.1. 「**十分性認定国**」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。

5.2. 「**AI システム**」とは、さまざまな自律性のレベルで動作するよう設計され、デプロイ後に適応性を示すことがあり、かつ、明示または黙示の目的のために、受け取ったインプットから、物理環境または仮想環境に影響を与えることがあるアウトプット（予測、コンテンツ、推奨、決定など）を生成する方法を推測する、機械ベースのシステムを意味します。

5.3. 「**連絡先個人情報**」（「**BCI**」）とは、管理上および契約管理の目的（例えば、請求およびアカウント管理、パートナー・インセンティブの計算、内部報告および事業モデル作成（予測、収益、能力計画など））で、職務上もしくは業務上の立場の個人に連絡し、これを特定し、またはこれを認証するために使用される個人データを意味します。典型的な例として、BCI には、個人の氏名、業務用電子メール・アドレス、実際の住所、電話番号その他同様の属性が含まれます。例えば、サポート・サービスのためにサプライヤーの関係者に連絡するために使用される氏名および電子メール・アドレスは、BCI に該当しますが、診断的サポート・データに含まれる氏名および電子メール・アドレスは、キンドリルの個人データに該当します。

5.4. 「**クラウド・サービス**」とは、サプライヤーがホストまたは管理する「サービスとしての」オファリングを意味し、これには、「サービスとしてのソフトウェア」、「サービスとしてのプラットフォーム」および「サービスとしてのインフラ」オファリングが含まれます。

5.5. 「**管理者**」とは、単独でまたは他者と共同で個人データの処理の目的および手段を決定する、自然人または法人、公的当局、機関その他団体を意味します。

5.6. 「**会社システム**」とは、キンドリルが自らの業務のために依拠する情報技術システム、プラットフォーム、アプリケーション、ネットワークなどを意味し、これには、キンドリルのイントラネット、インターネットなどに置かれているものや、これらを通じてアクセス可能なものが含まれます。

5.7. 「**お客様**」とは、キンドリルの顧客を意味します。

5.8. 「**データ輸入者**」とは、十分性認定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。

5.9. 「**データ主体**」とは、直接または間接的に特定することが可能な自然人を意味します。

5.10. 「**日**」とは、「営業」日と指定されない限り、暦日を意味します。

5.11. 「**デバイス**」とは、キンドリルが提供する、またはサプライヤーが提供する、ワークステーション、ノートパソコン、タブレット、スマートフォンまたは携帯情報端末を意味します。

5.12. 「**施設**」とは、サプライヤーが成果物またはキンドリル資料をホストし、それにアクセスし、その他その処理を行う物理的な場所を意味します。

5.13. 「**業界標準慣行**」とは、アメリカ国立標準技術研究所（「**NIST**」）または国際標準化機構（「**ISO**」）その他同様の評判および高度な知識を有する団体もしくは組織によって、推奨または要求される慣行を意味します。

5.14. 「**キンドリルのデータ**」とは、サービスまたは成果物の引渡しに関連して、クラウド・サービスなどを経由してサプライヤーに対して提供された、またはサプライヤーによるアクセスが可能になった一切のデータ、ファイル、資料、テキスト、音声、動画、画像その他のデータを意味し、キンドリルの個人データ、キンドリルのBCIおよびキンドリルの非個人データが含まれますが、キンドリル、キンドリルの関係者、お客様、お客様の従業員または契約者、その他の人または団体のいずれによって提供されたか、またはアクセス可能なったかを問いません。

5.15. 「**キンドリル資料**」とは、すべてのキンドリルのデータおよびキンドリルのテクノロジーを意味します。

5.16. 「**キンドリルの個人データ**」とは、サービスまたは成果物の引渡しのためにキンドリルがサプライヤーに提供するまたはサプライヤーによるアクセスを可能にする個人データ（キンドリルの BCI

を除く）を意味します。キンドリルの個人データには、キンドリルが管理する個人データおよびキンドリルがその他の管理者のために処理する個人データも含まれます。

5.17. **「キンドリルのテクノロジー」**とは、取引文書または本契約に関連して、キンドリルがサプライヤーに対して直接または間接的にライセンス許諾し、その他利用に供した、ソース・コード、他のコード、記述言語、ファームウェア、ソフトウェア、ツール、設計図、概略図、グラフ表示、埋込キー、証明書その他情報、資料、資産、文書およびテクノロジーを意味します。

5.18. **「非十分性認定国」**とは、適用されるデータ保護法または管轄権を有する規制当局の決定に従って適切であると認定されていない国を意味します。

5.19. **「その他の管理者」**とは、キンドリルを除き、キンドリルのデータの管理者である法主体（キンドリルの関係会社、お客様、お客様の関係会社など）を意味します。

5.20. **「オンプレミス・ソフトウェア」**とは、サプライヤーによって成果物として提供されるソフトウェアであって、キンドリルまたはキンドリルの従契約者のサーバーまたはシステム上で、キンドリルまたは従契約者が実行、インストールまたは操作するものを意味します。

5.21. **「個人データ」**とは、データ主体に関係する情報、その他データ保護法に基づく「個人データ」等に分類される情報を意味します。

5.22. **「関係者」**とは、キンドリルもしくはサプライヤーの従業員、キンドリルもしくはサプライヤーの代理人、キンドリルもしくはサプライヤーから委託された独立契約者に該当する個人、または従契約者によって当事者に提供された個人を意味します。

5.23. **「処理する」**または**「処理」**とは、キンドリルのデータに関して実施される操作または一連の操作（保存、使用、アクセスおよび読込みを含む）を意味します。

5.24. **「処理者」**とは、管理者に代わり個人データを処理する自然人または法人を意味し、データ保護法に基づく「サービス・プロバイダー」のほか、実質的に同様の用語を含みます。

5.25. **「セキュリティ・インシデント」**とは、(a) キンドリル資料またはサービスもしくは成果物を提供するためにサプライヤーもしくはその従契約者によって使用される情報システムの機密保持、完全性または可用性を、実際に脅かしているか、その危険が差し迫っている出来事、(b) 転送、保存その他の方法で処理されるキンドリルのデータに対する偶発的もしくは違法な破壊、紛失、改変、不正な開示またはアクセスにつながるセキュリティ侵害、(c) サービスもしくは成果物の引渡しにおいて、またはこれに関連して、サプライヤーまたはその従契約者によって使用されるソース・コードへの不正なアクセスまたはその使用を意味します。

5.26. **「販売する」**（または「**販売**」）とは、金銭その他価値ある対価と引き換えに、データを（口頭、書面、電子的その他の手段により）賃貸、リース、開示、配布、利用可能化、転送、その他伝達することを意味します。

5.27. **「共有する」**とは、2018 年カリフォルニア州消費者プライバシー法（2020 年消費者プライバシー権法により改正）に定める意味を有します。

5.28. **「標準契約条項」**（「**SCC**」）とは、十分性認定国で設立されていない管理者または処理者への個人データの転送に対して、適用されるデータ保護法により求められる契約条項を意味します。

5.29. **「ソース・コード」**とは、製品の作成、開発または保守において開発者によって使用される人間可読プログラミング・コード、または人間可読形式に変換可能なコードを意味します。これは、製品の通常の市販または商用の過程において公表されることはありません。

5.30. **「復処理者」**とは、キンドリルの個人データを処理する、サプライヤーの従契約者（サプライヤーの関係会社を含む）を意味します。

5.31. **「監督機関」**とは、特定の国または地域内においてデータ保護法の適用状況を監視する責任を負う、独立公共団体を意味します。