Kyndryl のデータのセキュリティーおよびプライバシーの原則

1. 定義

本書で使用される定義語の定義は以下のとおりです。以下に記載されていない場合には、Kyndryl とお客様の間で「Kyndryl サービス」に関して締結された該当する契約書に記載された定義のとおりとなります。

「お客様」とは、Kyndryl が「Kyndryl サービスに関する文書」に基づく「Kyndryl サービス」を提供する相手にあたる事業体になります。

「コンポーネント」とは、Kyndryl が運用および管理する、「Kyndryl サービス」のアプリケーション、プラットフォーム、またはインフラストラクチャーに関する要素になります。

「コンテンツ」は、お客様またはお客様の許可ユーザーが提供する、アクセス権限を与える、または「Kyndryl サービス」に入力する、すべてのデータ、ソフトウェアおよび情報で構成されます。

「DSP」とは、この「Kyndryl のデータのセキュリティーおよびプライバシーの原則」のことです。

「Kyndryl サービスに関する文書」とは、「個別契約書」、ならびに Kyndryl とお客様の間で締結された契約書に取り込まれるその他の文書、および特定の「Kyndryl サービス」の詳細に対処するその他の文書になります。

「Kyndryl サービス」とは、(a) Kyndryl がお客様に提供する、お客様に専用で提供する、もしくはお客様用にカスタマイズする、インフラストラクチャーまたはアプリケーションのサービス・オファリングを含む、Kyndryl サービス・オファリング、および (b) Kyndryl がお客様に提供するその他のサービス (コンサルティング、保守、またはサポートを含みます。) になります。

「セキュリティー・インシデント」とは、「コンテンツ」の不正アクセスおよび不正使用のことです。

「個別契約書」とは、料金、「Kyndryl サービス」の説明、および「Kyndryl サービス」についての情報など、取引の詳細が記載された文書になります。「Kyndryl サービス」のサービス仕様書、サービス記述書、注文書、および請求書などは、「個別契約書」の一例です。取引に適用される「個別契約書」は複数ある場合があります。

2. 概要

本 DSP に定められた技術的および組織的措置は、Kyndryl が、Kyndryl とお客様の間で締結された契約書で DSP を遵守することに明示的に同意した場合に限り、「Kyndryl サービス」(すべての「コンポーネント」を含みます。) に適用されます。明確にするために付言すると、お客様がセキュリティーおよびプライバシーに対して責任を負う場合、または以下もしくは「Kyndryl サービスに関する文書」に記載がある場合にはそれに従って、これらの対策は適用されません。

a. 「Kyndryl サービス」がお客様の使用に適しているかどうかの判断を行うこと、ならびに Kyndryl が「Kyndryl サービス」内で提供したり管理したりしないコンポーネントに対しセキュリティーとプライバシーの対策を実施し、管理することについて、お客様は責任を負います。「Kyndryl サービス」に対してお客様が負う責任の例は次のとおりです。(1) Infrastructure as a Service (IaaS) もしくは Platform as a Service (PaaS) のオファリング上で、または Kyndryl がお客様に代わって管理するインフラストラクチャー、「コンポーネント」、もしくはソフトウェア上で、お客様が構築または展開したシステムおよびアプリケーションのセキュリティー、ならびに (2) Kyndryl がお客様の代わりに管理する Software as a Service (SaaS) オファリング、または Kyndryl がお客様に提供するアプリケーション・サービス・オファリングに関する、お客様のエンド・ユーザーのアクセス制御およびアプリケーション単位のセキュリティー構成。

b. お客様は、Kyndryl が自己裁量で本 DSP を随時変更でき、かかる変更が、Kyndryl が修正版を公開した日付で旧版に取って代わることを了承します。Kyndryl とお客様の間で締結されたいずれかの契約書の相反する規定にかかわらず、変更は次のいずれかを意図して行われます。(1) 既定の義務を改善もしくは明確化すること、(2) Kyndryl が進化するデータおよびサイバーセキュリティーに関する脅威や問題に対処するため適切にセキュリティーの優先順位付けを行えるようにすること、(3) 最新の採用されている基準および適用法との整合を維持すること、または (4) 追加機能を提供する

こと。変更によって、「Kyndryl サービス」のセキュリティーまたはデータ保護機能が低下することはありません。

c. 本 DSP と「Kyndryl サービスに関する文書」の間になんらかの矛盾が生じた場合には、「Kyndryl サービスに関する文書」が優先し、「個別契約書」に矛盾する条件がある場合には、当該条件は本 DSP の条件をオーバーライドするものとして指定され、該当する特定の取引にのみ適用されます。

3. データ保護

a. Kyndryl はすべての「コンテンツ」を機密として取り扱い、「Kyndryl サービス」を提供するために必要な範囲に限り、Kyndryl の従業員、従契約者、サプライヤー (復処理者を含みます。) に開示する場合を除き、「コンテンツ」を開示しません。

b. 各「Kyndryl サービス」に対するセキュリティーとプライバシーの対策は、Kyndryl のセキュリティーおよびプライバシー・バイ・デザインの慣例に従って実装され、「Kyndryl サービス」で処理される「コンテンツ」を保護し、Kyndryl とお客様の間で締結された該当する契約書 (「Kyndryl サービスに関する文書」を含みます。) に従ってかかる「コンテンツ」の可用性を維持します。

c. 「Kyndryl サービス」の使用の適合性に関するお客様による初期評価および継続評価を支援するため、「Kyndryl サービス」に固有のセキュリティーとプライバシーに関する追加情報が、関連する「Kyndryl サービスに関する文書」またはその他の標準文書で提供される場合があります。かかる情報には、公にされた認証および認定の証拠、かかる認証および認定に関連する情報、データ・シート、FAQ、およびその他一般に入手可能な文書が含まれます。お客様が希望するセキュリティーとプライバシーに関するアンケートに回答するよう依頼があった場合、Kyndryl は、お客様に利用可能な標準文書を案内します。

4. セキュリティー・ポリシー

a. Kyndryl は、Kyndryl のビジネスに不可欠であり、かつ Kyndryl の全従業員に義務付けられる IT セキュリティー・ポリシーおよび慣例を書面で維持し、これに従います。Kyndryl の最高情報セキュリティー責任者は、かかるポリシーについて常に責任を負い、幹部として監督します。これには、正式なガバナンスおよび改正の管理、従業員教育、ならびに法令遵守の徹底が含まれます。

b. Kyndryl は、自社の IT セキュリティー・ポリシーを少なくとも年 1 回見直し、「Kyndryl サービス」および「コンテンツ」の保護を維持するために Kyndryl が相応と判断する場合、かかるポリシーを修正します。

c. Kyndryl は、新規採用者全員について、自社の標準の必須の雇用検証要件を維持し、これに従います。また、当該要件の遵守を Kyndryl の完全子会社にも拡大して適用します。Kyndryl の社内プロセスおよび手続きに従って、これらの要件は定期的に見直されます。また雇用確認要件には、犯罪歴の確認、身元確認の証拠、および Kyndryl が必要とみなすその他の確認が含まれます。Kyndryl のグループ会社は、その必要性と現地法で許される範囲で、適宜その採用プロセスに上記の要件を組み込む責任を負います。

d. Kyndryl の従業員は、年 1 回、Kyndryl のセキュリティーとプライバシーに関する教育を履修し、Kyndryl の「ビジネス・コンダクト・ガイドライン」に規定された倫理的な行動基準、守秘義務、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します。「コンポーネント」への特権アクセスが付与されているユーザーには、「Kyndryl サービス」に関する Kyndryl の運用およびサポートにおける各自の役割に固有の追加トレーニングが、関連する「Kyndryl サービスに関する文書」に記載された準拠および認証を維持するのに必要な内容に応じて、提供されます。

5. 遵守

a. Kyndryl は「Kyndryl サービスに関する文書」に定義されているとおりに「Kyndryl サービス」の適合性および認証を維持します。

b. Kyndryl は要求に応じて、認定されている独立第三者監査の結果として得られる証明書、証書、またはレポートなど、第 5a. 項で義務付けられている適合性と認証の証拠を提供します (認定されている独立第三者監査は関連基準に義務付けられている頻度で実施されます。)。

c. Kyndryl が従契約者またはサプライヤー (復処理者を含みます。) を「Kyndryl サービス」の提供およびサポートで使用する場合、Kyndryl はこうしたデータのセキュリティーとプライバシーの対策に責任を負います。

6. セキュリティー・インシデント

a. Kyndryl 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関する National Institute of Standards and Technology, United States Department of Commerce (NIST) のガイドラインまたは同等の業界基準に合致する、文書化されたインシデント対応ポリシーを維持し、それに従い、Kyndryl とお客様の間で締結された該当する契約書に記載されたデータ漏えいの通知に関する条件を遵守します。

b. Kyndryl は、Kyndryl が気付いた「セキュリティー・インシデント」を調査し、「Kyndryl サービス」の適用範囲内で、Kyndryl は適切な対応計画を作成して実行します。脆弱性やインシデントが疑われる場合に、お客様が Kyndryl に通知するには、「Kyndryl サービス」固有のインシデント・レポート・プロセス (「Kyndryl サービスに関する文書」に記載のとおり) を通じて要求を提出するか、かかるプロセスがない場合にはテクニカル・サポート要求を提出します。

c. Kyndryl は、Kyndryl がお客様に影響が及ぶことを把握しているか、合理的な範囲でそのような疑いを持っている「セキュリティー・インシデント」について、それを確認したらすぐに、不当な遅滞なく、お客様に通知します。Kyndryl は、かかる「セキュリティー・インシデント」ならびに Kyndryl による修復作業および回復作業の状況について、合理的な範囲で要求された情報をお客様に提供します。

7. 物理的セキュリティーおよび入場管理

a. Kyndryl は、「Kyndryl サービス」をホストするために使用される Kyndryl 管理施設 (データセンター) への無許可入場を防止するため、現場での適切な入場管理 (柵の設置、入口でのカードによる入退制限、監視カメラ、および有人の受付デスクなど) を実施します。配達エリアや発送センターなど、かかるデータセンターにつながる入口は管理され、コンピューティング・リソースから隔離されます。

b. Kyndryl が管理するデータセンターおよび当該データセンター内の管理エリアへのアクセスは、職務別に制限され、正当な承認が必要になります。かかるアクセスはログに記録され、かかるログは 1 年以上保持されます。アクセス権限のある従業員が離職した場合、Kyndryl は離職直後に、Kyndryl が管理するデータセンターへのアクセス権限を無効にします。Kyndryl 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。

c. Kyndryl が管理するデータセンター施設、またはかかるデータセンター内の管理エリアに入場する一時的な許可を付与された個人は全員、当該施設に入場する際に登録され、登録時に身分証明書の提示が義務付けられ、権限ある要員が付き添います。搬出・搬入を含む、入場のための一時的な許可は、事前の計画および権限ある承認を必要とします。

d. Kyndryl は、Kyndryl が管理するデータセンター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。

8. アクセス、介入、転送、および分離の管理

a. Kyndryl は、当該ネットワーク・アーキテクチャーの安全な分割、分離、および多層防御の基準を遵守するために、これを実装する前に、「コンポーネント」用のセキュリティー・アーキテクチャーを精査します。これには、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ぐための対策が含まれています。

b. Kyndryl は、「Kyndryl サービス」および関連する「コンポーネント」の保守およびサポートにおいて、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。かかる無線ネットワークを使用する場合は暗号化され、セキュア認証が必要になります。

c. Kyndryl は、「コンテンツ」がアクセス権限のない個人に公開される、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されそれらの事象を防止するように設計された「Kyndryl サービス」のための対策を維持します。Kyndryl は、実稼働環境と非実稼働環境の適切な分離を維持し、例えばお客様の要求に応じてエラーを再現するためなど、「コンテンツ」が非実稼働環境に転送される場合は、非実稼働環境におけるセキュリティーおよびプライバシーの保護対策は、実稼働環境における保護対策と同様に設定されます。

d. Kyndryl は、お客様がパブリック・ネットワークを介して「コンテンツ」を「Kyndryl サービス」との間で安全に転送できるようにするために、公開表示または権限のない閲覧を意図しない「コンテンツ」をパブリック・ネットワークで転送する際に「コンテンツ」を暗号化し、暗号プロトコル (HTTPS、SFTP、または FTPS など) を使用可能にします。

e. Kyndryl は、「Kyndryl サービスに関する文書」に明記されている場合は明記されているとおりに、保存されている「コンテンツ」を暗号化します。「Kyndryl サービス」に暗号鍵の管理が含まれる場合、Kyndryl は、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。

f. Kyndryl が「Kyndryl サービス」を提供するために「コンテンツ」へのアクセスを必要とする場合で、かかるアクセスが Kyndryl によって管理される場合、Kyndryl は必要な最低限のレベルにアクセスを制限します。基盤となる「コンポーネント」への管理者アクセス (特権アクセス) を含め、かかるアクセスは、個人用の、役割ベースのもので、職務分離の原則に従って権限のある Kyndryl 要員が行う承認および定期的な検証を受けます。Kyndryl は、特権的アクセス権の付帯する重複アカウントおよび休止アカウントを特定し、削除するための手段を維持管理します。また、アカウント所有者の離職にあたって、または権限のある Kyndryl 要員 (アカウント所有者のマネージャーなど) の要求に応じて、当該アクセス権限を速やかに取り消します。

g. 業界標準の慣例に合わせて、かつ各「コンポーネント」でネイティブにサポートされている範囲に限り、Kyndryl は、非アクティブ・セッションのタイムアウト、アカウントのロックアウト (ログインが連続して複数回失敗した後に実行される)、強力なパスワードまたはパスフレーズによる認証、パスワード変更の頻度、ならびにかかる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強制する技術的な対策を維持します。

h. Kyndryl は、特権的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対策を維持します。(1) 不正アクセスおよび不正なアクティビティーの特定、(2) タイムリーかつ適切な対応の促進、ならびに (3) 文書化された Kyndryl ポリシーへの準拠に関する社内監査および独立した第三者による監査の実施。

i. 特権的なアクセスおよびアクティビティーが記録されたログは、Kyndryl のポリシーに従って保存されます。Kyndryl 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ことを目的として設計された対策を維持します。

j. ネイティブ・デバイスまたはオペレーティング・システムの機能のサポート対象となっている範囲において、Kyndryl は、エンド・ユーザー・システムのコンピューティング保護を維持します。これには以下のものが含まれますが、これらに限定されません。すなわち、エンドポイント・ファイアウォール、フルディスク暗号化、マルウェアの検出および削除、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。

k. Kyndryl は、メディアのサニタイズに関する NIST のガイドラインに従って、再利用を意図している物理メディアのサニタイズを再利用する前に安全に行い、再利用を意図していない物理メディアは破棄します。

9. サービスの完全性および可用性管理

a. Kyndryl は以下をすべて行います。(1) 「Kyndryl サービス」のセキュリティーとプライバシーのリスク・アセスメントを年 1 回以上実施する、(2) 実稼働リリース前に「Kyndryl サービス」のセキュリティー・テストと脆弱性評価を実施し、実稼働リリース後は年 1 回以上実施する、(3) 実稼働リリース前およびその後は年 1 回、機能とオファリングに関して侵入テストを実施する、(4) 業界のセ

キュリティー構成のベスト・プラクティスに照らして、「Kyndryl サービス」の基盤となる「コンポーネント」の自動脆弱性スキャンを実行する、(5) 関連リスク、悪用可能性、影響などに応じて、セキュリティー・テストおよびスキャンから特定された脆弱性を修復する、(6) テスト、評価、スキャン、および修復作業などの実行時に、「Kyndryl サービス」の中断を回避するために合理的な範囲の対策を講じる。

b. Kyndryl は、「Kyndryl サービス」、ならびに「Kyndryl サービス」の適用範囲内で関連するシステム、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」を評価してテストし、セキュリティー・アドバイザリー・パッチを適用できるように設計された対策を維持します。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、Kyndryl は、重大度およびリスク・アセスメントに関する文書化されたガイドラインに従い、該当する場合にはパッチの「共通脆弱性評価システム」レーティングに基づいて、当該パッチを実装します。セキュリティー・アドバイザリー・パッチの実装は、Kyndryl の変更管理ポリシーに従って行われます。

c. Kyndryl は、「Kyndryl サービス」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。実装前に、「Kyndryl サービス」(そのシステム、ネットワーク、および基盤となる「コンポーネント」を含みます。) に対する変更は登録済みの変更要求に記録されます。この変更要求には、変更の説明および理由、実装の詳細およびスケジュール、「Kyndryl サービス」およびそのユーザーへの影響に対処するリスク・ステートメント、予期される結果、ロールバック計画、ならびに権限のある担当者による文書での承認が含まれます。

d. Kyndryl は、「Kyndryl サービス」の運用において使用されるすべての情報技術資産のインベントリーを維持管理します。Kyndryl は、「Kyndryl サービス」および基盤となる「コンポーネント」の健全性 (キャパシティーを含みます。) および可用性を継続的にモニターし、管理します。

e. 各「Kyndryl サービス」は、事業継続性および災害復旧の要件に対して個別に評価されます。この際、重要なビジネス機能を特定して優先順位を付けるため、適切なビジネス・インパクト分析およびリスク・アセスメントが行われます。各「Kyndryl サービス」には、かかるリスク・アセスメントで保証される範囲で、業界標準の慣例に合致する事業継続性計画および災害復旧計画が付帯します。こうした計画は、個別に定義され、文書化され、維持され、年 1 回検証されます。「Kyndryl サービス」の目標復旧時点および目標復旧時間が、関連する「Kyndryl サービスに関する文書」に定められている場合は、「Kyndryl サービス」のアーキテクチャーおよび使用目的を考慮して設定されます。「Kyndryl サービス」のバックアップ・ファイルが保存されたメディアなど、オフサイト・ストレージを意図した物理メディアがある場合は、転送前に暗号化されます。