サプライヤー管理義務（SCO）

管理要件 -

情報、サイバーおよび物理的セキュリティー、テクノロジー、復旧計画、データプライバシー、データ管理、および EUDA

MC 1.0 - ガバナンスおよび説明責任

サプライヤーは、情報技術、情報技術セキュリティー、物理的セキュリティー、復旧計画、データ管理および個人情報管理（データプライバシー/データ保護）ガバナンス（NIST、ISO/IEC 27001、COBIT、BS10012、SSAE 18、ITIL）に関する確立された一貫性のある業界標準フレームワーク、または同様の業界のベストプラクティス標準フレームワークを使用し、そのプロセス、テクノロジー、物理環境の安全保護または対策の効果的な実施を確認する必要があります。十分に構造化された全社規模のガバナンスプログラムにより、可用性、完全性、機密性という核となる概念が適切な管理によってサポートされるていることを確認する必要があります。上記の管理は、情報の損失、破壊または破損のリスクを緩和または低減するように設計されている必要があり、サプライヤーは Barclays に提供されるサービスを保護するために、Barclays の要件を満たす管理の適用と、効果的な運用を確認する必要があります。

ガバナンスフレームワークを策定し、偶発的および/または意図的な損失、開示、改変または破壊、盗難、不適切な使用もしくは誤用、ならびに不正なアクセス、使用または開示から資産および情報/データを保護するための管理運営、技術および物理的な安全保護を含める必要があります。

ガバナンスおよび説明責任プログラムには以下を含める必要がありますが、これらに限定されません。

- 管理者は、ガバナンスに関する方針（ガバナンスに関する一連の方針）を定義、承認し、これをサプライヤーの従業員および関連当事者に公開・伝達し、維持するものとします。
    - 方針および標準の実施の有効性を効果的に策定・実施・継続測定する方針、手続および標準的なプログラム。
    - 説明責任と啓発の文化を育成するための、明確なリーダーシップ構造と経営陣の監督下にある包括的なガバナンスプログラム。
    - 組織全体で承認された方針と手順の継続的な伝達。
    - 法的要件に適合する方針、慣行、計画的なデータ保護、および方針やプロセスの効果的な導入を確保するためのその他の管理
- ガバナンス方針とメカニズムの見直しと監視を行い、管理することで、方針およびプロセスが効果的に実施されるようにします。
- あらゆる分野の方針について、継続的な適合性、妥当性および有効性を確保するため、計画された時期に、または重大な変更が発生した場合に見直しを行う必要があります。
    - 方針および手順/標準の定期的な見直しの確保（少なくとも年１回、または重要な変更があったときのいずれか早い時点）。
- 役割および責任 - 責任を定義し、割り当てを行います。
    - 情報資産に対する個人の説明責任および所有権

    - Barclays が物理的および建物の安全性、情報、サイバーセキュリティーおよび個人情報管理（データプライバシー/データ保護）に関して連携することができる、方針、慣行、計画的なデータ保護、その他の管理の効果的な実施および監視について責任を負う経験豊富な適格者を任命すること。
    - サプライヤーは、内部および下請業者/復処理者を使用して管理の有効性を実装、管理および監督する人員の役割と責任を調整し整合させる必要があります。
- サプライヤーは、組織をあらゆる脅威（サイバーセキュリティーを含む）から保護するために、安全なインフラと管理のフレームワークを導入する必要があります。
- 独自の見直しおよび評価 - 情報セキュリティーアーキテクチャプログラム（すなわち、情報セキュリティーに関する管理目標、管理、方針、プロセスおよび手順）の管理および実施に対するサプライヤーのアプローチについて、計画された時期に、または重大な変更が発生した場合に、独自の見直しを行います。
    - 少なくとも年に 1 度、独自に見直しと評価を行い、確立された方針、基準、手順、およびコンプライアンス義務に対する不適合に組織が対処できるようにする必要があります。
    - 情報システムは、組織が情報セキュリティー方針および基準に継続的に準拠するよう、少なくとも毎年見直します。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドコンピューティングに関する情報セキュリティーポリシーは、クラウドサービス利用者のトピック固有の方針として定義します。クラウドサービス利用者のクラウドコンピューティングに関する情報セキュリティーポリシーは、情報やその他の資産に関する組織の許容可能なレベルの情報セキュリティーリスクと一致しているものとします。クラウドコンピューティングに関する情報セキュリティー方針を定義する場合、クラウドサービス利用者は次の点を考慮するものとします。

- クラウドコンピューティング環境に保存された情報は、クラウドサービスプロバイダーによるアクセスと管理の対象となる可能性があること。
- 資産がアプリケーションプログラムなどのクラウドコンピューティング環境内で保持される場合があること。
- マルチテナントの仮想クラウドサービス上でプロセスが実行可能であること。
- クラウドサービスユーザー、および当該ユーザーがクラウドサービスを使用する背景。
- クラウドサービス管理者がクラウドサービス利用者に特権的にアクセス可能であること。
- クラウドサービスプロバイダーの組織の地理的位置、およびクラウドサービスプロバイダーがクラウドサービス利用者データ（一時ストレージを含む）を保存する可能性のある国。

クラウドサービス利用者の関連するセキュリティー方針では、クラウドサービスプロバイダーをサプライヤーの一種として特定し、セキュリティー方針に従ってそれらを管理します。上記は、クラウドサービスプロバイダーに関連するクラウドサービス利用者データへのアクセスと管理によって生じるリスクを軽減することを目的としています。

クラウドサービス利用者は、クラウドサービス利用者に適用される法律に加え、クラウドサービスプロバイダーに適用される法域の関連法および規制を考慮する必要があります。クラウドサービス利用者は、クラウドサービス利用者の業務に必要なクラウドサービスプロバイダーによる関連規制や規格の遵守の証明を取得する必要があります。上記の証明には、第三者監査人が作成した誓約書/証明書も含まれます。

合併、買収、その他の所有権の変更があった場合、サプライヤーは、法的に可能な限り速やかに Barclays に書面により通知する必要があります。

MC 2.0 - リスク管理

サプライヤーは、サプライヤーが管理する環境全体のリスクを効果的に評価、低減、監視するリスクマネジメントプログラムを策定する必要があります。

リスクマネジメントプログラムには以下が含まれる必要がありますが、これらに限定されません。

- サプライヤーはリスク管理フレームワーク（情報、サイバー、物理的、テクノロジー、データおよび復旧計画など）を策定する必要があります。フレームワークは、適切な監督機関（取締役会またはその委員会など）によって承認される必要があります。これは、事業戦略やリスクマネジメントのフレームワーク全体に採用されている必要があります。
- リスクフレームワークに沿って、正式なリスク評価は、少なくとも年に 1 度、または計画された間隔で、リスクベースの手法により実施されるものとし、また、例えば、情報システムまたは物理的な建物や空間の変更があった場合に関連して、インシデントまたはそれに関連した教訓など何らかの事案に対応し、定性的かつ定量的な方法を用いて、特定されたすべてのリスクの発生見込みと影響を判断する必要があります。固有リスクおよび残存リスクに関連する発生見込みおよび影響は、すべてのリスクカテゴリー（監査結果、脅威と脆弱性の分析、規制遵守など）を考慮し、独自に決定するものとします。
- 以下を含むリスク基準を確立および維持する：
    - リスク受容基準
    - リスク評価の実施基準
- リスクを特定する：
    - リスク評価プロセスを適用して、リスクフレームワークの範囲内で情報の機密性、完全性、可用性の喪失に関連するリスクを特定する
    - リスクオーナーを特定する
- リスクを分析する：
    - リスクが特定された場合に生じ得る結果を評価する

- 特定されたリスクが発生する可能性を現実的に評価する
- リスクのレベルを決定する

- リスクを評価する：
  - リスク分析の結果を確立されたリスク基準と比較する
  - リスク処理のために分析済みリスクを優先順位化する
- リスク処理：
  - リスク評価の結果を考慮し、リスクに対する適切な対応方法を選択する
  - 選択したリスク処理オプションを実施するために必要なすべての管理を決定する
  - 実施の有無にかかわらず、必要な管理および実施の根拠を含む適用宣言書を作成する
  - サプライヤーは、リスクに優先順位を付け対策を講じることにより、特定の状況下におけるリスクを確実に最小化または排除する必要があります。サプライヤーは継続的に対策を監視し、それらが効果的であることを確認する必要があります。
- サプライヤーは、情報、サイバー、物理的セキュリティー、データプライバシー/データ保護および復旧計画に関連して、最低でも年 1 回のリスク評価を実施する必要があります。現在および新たな脅威が存在する特定の環境に基づいて、サプライヤーはより頻繁な頻度での発生を考慮する必要があります。
  - Barclays に提供されるプロセス/サービス（データセンターを含む）の運営に不可欠なサイトを少なくとも年に 1 回評価する
- 組織は、情報セキュリティーリスク評価プロセスに関する文書化された情報を保持するものとします。
- データガバナンス要件に関するリスク評価については、以下の点を考慮する必要があります。
  - データを分類し、不正使用、アクセス、紛失、破壊、改ざんから保護する。
  - アプリケーション、データベース、サーバー、ネットワークインフラストラクチャ間で機密データがどこに保存され、転送されているかを確認する。
  - 定義された保管期間および使用期間経過後の破棄に関する要件を遵守する。
- サプライヤーはプライバシー影響評価を実施し、そのようなプライバシーリスクが、ミッション、機能、他のリスク管理の優先事項（コンプライアンス、財務など）、評判、労働力、文化など、組織の業務にどのような後続的影響が生じる可能性があるかを確認する必要があります。
- サプライヤーは、プライバシーリスクによって通知される組織のリスク管理の優先順位を継続的に理解できるように、組織のガバナンス構造を策定し導入する必要があります

サプライヤーは、Barclays に提供するサービスに重大な影響を与える可能性のあるリスクを低減または排除できない場合は、Barclays に通知する必要があります。こうした事例は、規制当局の報告義務を遵守するため、発見から 10 営業日以内に速やかに Barclays に報告する必要があります。

MC 3.0 - 役割と責任

サプライヤーは、Barclays にサービスを提供する請負業者、下請業者、復処理者を含むがこれらに限定されないそのすべての従業員が Barclays の規制要件を認識し、当該要件に従うことについて責任を負います。サプライヤーは、Barclays の管理要件をサポートおよび/または管理するために、相応かつ適切なスキルを備え、明確な役割と責任を有する専門家および/または個人から成る適切なチームが配置され、Barclays のサービスを保護するために効果的に機能するようにする必要があります。

サプライヤーは、Barclays の管理要件を効果的にサポートする役割と責任を定義し、連絡調整を行わなければなりません。役割と責任は定期的に（少なくとも 12 ヵ月に 1 回）見直さなければなりません。また、サプライヤーの運営モデルまたは業務に重大な変更があった場合には、その都度見直さなければなりません。

サプライヤーは、その従業員、請負業者、下請業者/復処理者が、本基準および関連する方針および基準の管理要件を十分に理解し、遵守していることを確認する責任があります。管理要件の不遵守に起因する上申のために、サプライヤーは Barclays との連絡担当者を任命する必要があります。具体的な契約要件について、サプライヤーの下請業者/復処理者に書面で周知する必要があります。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者は、情報セキュリティーに関する役割と責任の適切な割り当てについてクラウドサービスプロバイダーと合意し、自らが割り当てられた役割と責任を果たすことができることを確認する必要があります。両当事者の役割と責任は、契約書に定める必要があります。クラウドサービス利用者は、そのクラウドサービスプロバイダーのカスタマーサポートおよびケア機能との関係を特定し、管理する必要があります。

クラウドサービス利用者は、クラウドサービスの利用に応じて既存の方針と手順を定義または拡大し、クラウドサービスの利用におけるその役割と責任をクラウドサービスのユーザーに知らせる必要があります。

MC 4.0 - 教育および意識向上

サプライヤーは、契約社員、短期雇用者、コンサルタントを含むすべてのサプライヤーの従業員を対象とした、継続的な意識向上トレーニングプログラムを実施する必要があります。Barclays のデータ/情報またはその他の物理的資産にアクセスできるすべての個人は、組織内の専門的能力に関連して、適切なトレーニングを受け、組織の方針、プロセスおよび手順についての最新情報を定期的に取得する必要があります。トレーニングおよび意識向上については、サプライヤーの従業員が各自の役割を安全に実行できる水準で準備する必要があります。実施するプログラムの記録については、適切な学習管理プラットフォームまたは手動プロセスで記録する必要があります。

サプライヤーは、Barclaysのサービスへの**加入後1ヵ月**以内および/またはBarclaysのサービスへの加入時に、すべてのサプライヤーの従業員が必須の教育および意識向上トレーニングを完了していることを確認する必要があります。当該トレーニングには、サイバーセキュリティー、物理的セキュリティー、復旧計画、個人情報管理（データプライバシー/データ保護）、データ管理、ITサービス管理、EUDA、およびBarclaysのデータの保護が含まれます。サプライヤーは毎年トレーニングを更新することに加え、サプライヤーの従業員がトレーニングおよび意識向上について理解していることを確認するテストを行わなければなりません。実施されるすべてのトレーニングは、Barclaysのサービスに従事するすべてのサプライヤーの従業員について記録および維持され、要求された場合はBarclaysに閲覧させなければなりません。

サプライヤーは、意識向上トレーニングプログラムに、ソーシャルエンジニアリングおよび内部脅威というサイバーセキュリティー関連トピックを含める必要があります。かかるリスクの脅威を明確に理解し、特定された問題を緩和するために、サプライヤーは企業レベルの全従業員に対してフィッシングシミュレーションテストなどの技術を用いたソーシャルエンジニアリング攻撃のシミュレーションテストを実施し、継続的に監視することが推奨されます。

システムへの特権アクセス許可を持つ者や、高リスクまたは重要なスペースへのアクセス許可、あるいは機密性の高い事業に携わる者などのハイリスクグループ（開発者やサポートを含む特権的なユーザー、上級役員、情報セキュリティー担当者、第三者の利害関係者を含む）は、各自の役割と責任に応じて情報セキュリティーおよび物理セキュリティー状況の意識向上トレーニングを受ける必要があります。

すべての物理的セキュリティー担当者（サプライヤー、不動産所有者、外部サプライヤーによって雇用されているか否かを問わない）は、現地の法律に従い、認可されライセンスを受けたサービスプロバイダーを通じて雇用され、契約を締結する必要があり、その法域で必要とされる場合は、セキュリティー義務を負うための個人ライセンスを有する必要があります。物理的セキュリティー担当者は、各自の役割と責任に見合ったセキュリティートレーニングを受ける必要があります。実施されるすべてのトレーニングは文書化し、すべてのセキュリティー担当者についてトレーニング記録を維持し、要求された場合は Barclays に閲覧させなければなりません

サプライヤーは、データ処理に従事する第三者の人員が関連する方針、プロセス、手順、契約、組織のプライバシーバリューに準拠してプライバシー関連の職務と責任を効果的に遂行できるよう、これらの者にプライバシー意識向上教育に関するトレーニングを受けさせなければなりません。実施されるすべてのトレーニングは文書化し、すべての担当者についてトレーニング記録を維持し、要求された場合は Barclays に閲覧させなければなりません

サプライヤーは、データ管理（重要なデータ要素やサードパーティの管理アプリケーションの管理）における職務を効果的に遂行するよう従業員をトレーニングする必要があります。

サプライヤーの EUDA オーナーは、EUDA の責任を負うサプライヤーの従業員を特定し、少なくとも年に 1 回、各自の役割に適した教育および意識向上トレーニングを実施し、管理への適合性を示す証拠を保持する必要があります。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者は、クラウドサービスビジネスマネージャー、クラウドサービス管理者、クラウドサービスインテグレーター、クラウドサービスユーザー（関連する従業員および請負業者を含む）の意識向上、教育、トレーニングプログラムに次の項目を追加する必要があります。

- クラウドサービスの使用に関する基準と手順
- クラウドサービスに関連する情報セキュリティーリスクとそのリスクの管理方法
- クラウドサービスの使用に伴うシステムおよびネットワーク環境のリスク
- 適用される法規制上の考慮事項

クラウドサービスに関する情報セキュリティーの意識向上、教育、トレーニングプログラムは、事業部門を含む管理者および監督管理者に対して提供する必要があります。上記の取り組みは、情報セキュリティー活動の効果的な連携を支えるものです。

MC 5.0 - インシデント管理

サプライヤーは、インシデントおよびその根本原因をサプライヤー環境から効果的に管理、包含、除去/緩和する、確立されたインシデント管理フレームワークを策定する必要があります。

サプライヤーはインシデント/危機を Barclays に上申する手順を含めたインシデントおよび危機管理手順を策定する必要があります。インシデントが発生した場合にサプライヤーが効果的かつ効率的に対応できることを示すため、インシデント/危機対応チームとプロセスに対し、少なくとも年に 1 回テストを実施する必要があります。また、サプライヤーは、インシデントが発生した場合に既定のタイムライン内で連絡担当者に通知する能力をテストし、要求された場合は Barclays にこれを示すものとします。

サプライヤーは、サプライヤーの従業員の役割およびインシデントへの対処/管理のフェーズを定義した、十分に文書化されたインシデント対応計画を策定する必要があります。

- 責任および手順 - 管理責任および手順の策定により、インシデントへの迅速かつ効果的で秩序ある対応を確保する必要があります。
- インシデントイベントの報告 - インシデントイベントは、可能な限り速やかに適切な管理チャネルを通じて報告するものとします。報告メカニズムは、すべてのサプライヤーの従業員および請負業者が容易にアクセス可能である必要があります。
- インシデントイベントの評価 - インシデントイベントを評価し、適切な重要度、分類、要求される対応を決定する必要があります。
    - インシデントの分類 - インシデントの分類尺度を設定し、イベントをインシデントとして分類する必要があるか否かを決定します。インシデントの分類と優先順位付けは、インシデントの影響と範囲を特定するのに役立ちます。
- インシデントへの対応 - インシデントは、サプライヤーのインシデント管理の文書化された手順に従って対応する必要があります。
    - インシデント封じ込め - 人、プロセス、テクノロジーの能力を活用し、環境内のインシデントを迅速かつ効果的に封じ込める。
    - 脅威の除去/緩和 - 人、プロセス、テクノロジーの能力を活用し、セキュリティー上の脅威およびその構成要素を環境から迅速かつ効果的に除去/低減する。
- インシデントからの教訓 - インシデントの分析と解決から得た知識を使用し、将来的なインシデントの可能性または影響を低減する必要があります。
- 証拠の収集 - サプライヤーは、証拠として役立つ情報の識別、収集、取得および保存の手順を定義し、適用する必要があります。

インシデント後 - Barclays のサービスに混乱が生じた後、通常の事業活動レベルまでサービスが回復してから **4 暦週**以内に**インシデント後報告書**を Barclays に提出しなければなりません。報告書には少なくとも以下の検討項目を含めなければなりません：

- 状況にまつわるイベント
- インシデント/危機の管理方法
- 根本原因分析
- サプライヤーまたは Barclays により「リスクイベント」として分類されるものか（すなわち十分に重要であると思われるため、サプライヤーが周知の適切な方針に従って関連の利害関係者に通知/上申する必要があるか）
- 「行動リスク」になるものか（例えば、サプライヤーが Barclays の顧客と直接取り引きしているなど）
- サプライヤーに周知の Barclays の顧客救済
- 再発防止のための継続的な改善

- サプライヤーは、現在および過去の検出・対処実績から得られた教訓を取り入れ、可能な限り対応措置が改善されるように努める必要があります。

連絡手段 - サプライヤーは、インシデント/危機が発生した場合に、Barclays と連携して行動するための窓口担当者を任命する必要があります。サプライヤーは、時間外の連絡先、電話番号などを含め、窓口担当者の連絡先詳細に変更があった場合は Barclays に通知しなければなりません。

連絡先詳細には、名前、会社内での責任、役割、メールアドレス、電話番号を含める必要があります。

Barclays のサービス、Barclays のシステムまたは Barclays のデータに影響を及ぼすインシデントが発生したことをサプライヤーが確認した場合、サプライヤーは直ちに、いかなる場合にも **2 時間**以内に Barclays に通知するものとします。

Barclays 企業からの通知を受けた場合を含め、**サイバーインシデント**をサプライヤーが認識した場合、サプライヤーは直ちに、かついかなる場合にも適用法により義務付けられた時間内に、あるいはかかる要件が存在しない場合は、サイバーインシデントを認識してから **48 時間**以内にメール（gcsojoc@barclays.com）を送信して Barclays に通知し、可能な限り、以下を含む関連情報を提供するものとします。（a）影響を受ける Barclays のデータ記録のカテゴリーとおおよその数量、および該当する場合は影響を受けるデータ主体のカテゴリーと人数、（b）Barclays および該当する場合は影響を受けるデータ主体へのサイバーインシデントの影響ならびに見込まれる結果、ならびに（c）サプライヤーが実施したまたは実施する是正措置および軽減措置。

サプライヤー（またはサプライヤーの人員）のセキュリティー保護措置の不履行により、またはサプライヤーからの（もしくはサプライヤーの人員からの）もしくはサプライヤーを通じた（もしくはサプライヤーの人員を通じた）保護対象個人データへの不正アクセスにより、**保護対象個人データ**の盗難、不正使用もしくは開示が発生した場合（実際に発生したか、発生が疑われるか、そのような申立てがあったかを問わない）、あるいはサプライヤーまたはサプライヤー人員が所有または管理する保護対象個人データに損失、損害または破損が生じた場合、その他保護対象個人データの不正処理があった場合、サプライヤーは、関連するイベントを認識した後、可能な限り速やかに、かついかなる場合でも **24 時間**以内に、gcsojoc@barclays.com にメールを送信して Barclays に通知し、当該イベントに関して Barclays に全面的に協力し、援助を提供するものとします。これには、データ、時間、場所、インシデントの種類、影響、状況および実施した緩和措置などのすべての関連情報を提供することも含まれます。

下請業者/復処理者を使用してサービスを提供する場合、サプライヤーは、Barclaysのデータ/情報または資産を保有または処理するにあたり、Barclaysから合意を取得する必要があります。サプライヤーは、下請業者/復処理者と契約関係を結ぶ必要があり、下請業者/復処理者が、その処理および/また保持するBarclaysのデータを情報保護するために効果的に機能する類似の業界慣行標準フレームワークにより認証されていることを確認する必要があります。下請業者/復処理者にインシデントが発生した場合は、上記のインシデント通知に従うことを確認する必要があります。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者は、インシデント管理に関する責任の割り当てを確認し、クラウドサービス利用者がクラウドサービス顧客要件を満たしていることを確認する必要があります。クラウドサービス利用者は、以下を実施するためのメカニズムに関する情報をクラウドサービスプロバイダーに要求する必要があります。
- クラウドサービス利用者が自ら検出したインシデント/イベントをクラウドサービスプロバイダーに報告するため。
- クラウドサービス利用者がクラウドサービスプロバイダーによって検出されたインシデント/イベントに関するレポートを受け取るため。
- クラウドサービス利用者が報告された情報セキュリティーイベントの状況を追跡するため。

MC 6.0 - IT 資産マネジメント（ハードウェアおよびソフトウェア）

サプライヤーは、資産のライフサイクル全体を通じて、効果的な資産管理プログラムを実施する必要があります。資産管理は、取得から使用終了および/または安全な処分までの資産のライフサイクルを管理し、環境における全レベルの資産に対し、可視性と安全性を提供する必要があります。

サプライヤーは、Barclays へのサービス範囲に含まれるすべての拠点および/または地理的な場所にあるビジネス上重要な資産（サプライヤー、下請業者/復処理者の敷地内で運用される、または Barclays が提供する Barclays 機器を含む）の完全、正確かつ最新の目録を保管するとともに、情報資産の目録が最新、完全、正確であることを確認するため少なくとも年に 1 回のテストを実施し、要求に応じて Barclays にテスト結果を示さなければなりません。

資産管理プロセスは、以下の条件を満たす必要があります。

- 資産目録 - 情報および情報処理施設に関連する資産を特定し、かかる資産の目録を作成し、維持します。
    - サプライヤーは、将来的に情報を保存または処理できるよう、すべての IT ハードウェア資産の正確かつ最新の目録を管理する必要があります。
    - サプライヤーは、サプライヤーにホストされている Barclays の機器および/またはサプライヤーに提供された Barclays の IT 資産の正確かつ最新の IT 資産目録を保有する必要があります。

- 一次請け、二次請け、および三次請けの構造を持つサプライヤーは、最新で完全かつ正確な資産目録（デスクトップ、ラップトップ、ネットワーク機器、RSA トークン、または Barclays が提供する資産を含む）を保管する必要があります。
- サプライヤーは、Barclays のすべての資産（ハードウェアおよびソフトウェア）の照合を毎年実施し、Barclays（最高セキュリティーオフィスの ECAM チーム）にその結果を通知する必要があります。
- Barclays のサービス提供に必要な、導入されたすべての承認済みソフトウェア製品の最新の目録を維持し、各々のライセンスの条件に準拠します。
- クラウドサービス利用者の資産目録は、クラウドコンピューティング環境に保存されている情報と関連資産を考慮する必要があります。目録の記録には、クラウドサービスの識別情報など、資産の保管場所が示されている必要があります。

- 資産の所有 - 目録に維持されている資産は、所有されるものとします。
  - 情報資産は、分類、重要度、事業運営上の価値に基づいて保護されます。
- 資産の許容可能な使用 - 情報および情報処理施設に関連する資産の許容可能な使用に関する規則は、明確化し、文書化し、導入する必要があります。
  - 不正な資産がネットワークから削除されていることを確認します。
  - サプライヤーは、リスクを排除するため、サポートされていない技術の低減、ならびに資産およびデータの使用期間満了、使用終了、および安全な処分のための効果的かつ効率的な手順を確実に実施する必要があります。
  - サポートのないソフトウェアとハードウェアに、目録システム上で「サポートなし」タグを付けます。
- 資産の返還 - すべてのサプライヤーの従業員および下請業者/復処理者（Barclays に提供するサービス範囲内）は、雇用、契約または合意の終了時に、所有しているすべてのサプライヤーの資産を返却するものとします。
  - Barclays の資産の「紛失または盗難」については、インシデント管理に従って調査し、Barclays に報告する必要があります。
  - サプライヤーの資産の「紛失または盗難」に Barclays の情報が含まれる場合は、インシデント管理に従って Barclays に報告する必要があります。

サプライヤーは、直接または間接を問わず、製品にセキュリティー脆弱性がある場合を含め、Barclays へのサービス提供に使用する IT 資産のサポート提供能力に周知の変更がある場合、これを Barclays に直ちに知らせ、これらの IT 資産の適時のアップグレードまたは撤去を行う必要があります。

Barclays の資産の移送 - サプライヤーは、Barclays のすべての資産およびデータが、それらが移送される脅威環境の影響を含め、移送される資産およびデータの分類および価値（財務的損害および風評被害の観点から）に見合った適切な管理が行われており、安全に移送されていることを確認するものとします。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者の資産目録は、クラウドコンピューティング環境に保存されている情報と関連資産を考慮する必要があります。目録の記録には、クラウドサービスの識別情報など、資産の保管場所が示されている必要があります。

商用ライセンスソフトウェアをクラウドサービスにインストールした場合、ソフトウェアのライセンス条項に違反する可能性があります。クラウドサービス利用者は、クラウドサービスにライセンスソフトウェアをインストールする前に、クラウド固有のライセンス要件を確認する手順を定める必要があります。クラウドサービスが柔軟で拡張性があり、ライセンス条項で許可されているよりも多くのシステムまたはプロセッサコアでソフトウェアを実行できる場合は、特に注意が必要です。

MC 7.0 - 物理的資産の安全な廃棄/破壊と電子情報のデータ残存

物理的および/または電子的な形態で保存された、サービスに使用される画像を含む Barclays の情報資産は、適切かつ安全な方法で破壊または消去し、Barclays のデータが復元可能でないことを検証する必要があります。

サプライヤーは、Barclays のデータをすべてのストレージメディアから安全に除去/消去および復元するためのデータ消去、パージング、破棄を含むがこれに限定されない、適切なサニタイズ方法を使用して、安全に廃棄するための業務プロセスおよび技術的措置をサポートする手順を定め、また、既知のコンピューターフォレンジック手段によって Barclays のデータを復元できないようにする必要があります。

Barclaysの媒体に格納されたデータは、セキュアワイプ、パージング、データ消去、資産破壊などの適切なデータ消去技術を使用するか、データを上書きするソフトウェアに基づいた方法、またはデータ廃棄に関する業界標準フレームワーク （NIST）を使用して、データが復元できないように消去しなければなりません。すべての機器（情報資産）は、耐用年数および/または運用期間の終了時に廃棄する必要があります（故障、廃止、または不要となったために廃棄する、試験または概念実証で使用した場合、再利用する機器にデータ消去サービスが利用できる場合など）。

廃棄要件は、Barclays へのサービス提供に使用するサプライヤーの下請業者/復処理者に適用されます。

ハードコピー情報の廃棄の際は、クロスカットシュレッダー（支払いカード情報を含む）を使用して少なくともP4 DIN 66399の基準までシュレッダーで破断処理するか、またはBS EN 15713:2009に準拠して焼却する必要があります。

Barclays に関しては、データの廃棄に関する証拠を保持し、監査記録、証拠、追跡を提供し、以下を含めなければなりません。

- 破壊および/または廃棄の証明（実施日および方法を含む）
- 削除に関するシステム監査記録。
- データ廃棄証明。
- 廃棄を実行した担当者（廃棄の際の共同作業者、第三者、請負業者を含む）。

- 破壊/削除処理の成否を確認するために、破壊および検証レポートを作成する必要があります。（すなわち、上書き処理では消去できなかったセクターの詳細を示すレポートを作成する必要があります）。

サプライヤーは、Barclays のための業務終了時に、Barclays からの通知と承認に基づいて Barclays のデータが安全に破棄されるようにしなければなりません。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者は、クラウドサービスプロバイダーがリソースの安全な廃棄または再利用のための方針と手順を定めていることの確認を要求する必要があります。クラウドサービス利用者は、クラウドサービス利用者の資産の返却と削除およびクラウドサービスプロバイダーのシステムからのすべての資産のコピーの削除を含む、サービス終了プロセスの文書化された説明を要求する必要があります。説明において、すべての資産をリストアップし、サービス終了のスケジュールを文書化する必要があり、これは適時に行われる必要があります。

MC 8.0 - 情報の分類とデータの取り扱い

サプライヤーは、以下を含む確立された適切な情報分類およびデータ取り扱いのフレームワークまたはプログラム（業界の最良慣行および/または Barclays の要件に従う）を備えている必要があります。

- 情報の分類 - 情報は、重要性および不正な開示または変更に対する感度の観点から分類されるものとします。
- 情報のラベリング - 情報のラベリングのための適切な一連の手順は、サプライヤーが採用した情報分類スキームに従って作成および実施するものとします。
- 資産の取扱い - 資産の取扱い手順は、サプライヤーが採用した情報分類スキームに従って策定し、実施するものとします。
- すべてのスタッフが、サプライヤー/Barclays のラベリングと取り扱い要件、および正確な情報分類を正しく適用する方法を認識していることを確認します。

サプライヤーは、Barclays の情報ラベリングスキームおよび取り扱い要件（付録 A、表 A1 および A2）またはその代わりとなるスキームを参照し、保持および/または処理された Barclays の情報を保護および安全に管理する必要があります。この要件は、下請業者/復処理者を含め、Barclays に代わって保有または処理されるすべての Barclays の情報資産に適用されます。

クラウドサービス利用者（サプライヤー）向けガイダンス

クラウドサービス利用者は、クラウドサービス利用者が採用しているラベリング手順に従って、クラウドコンピューティング環境で維持されている情報と関連資産にラベリングを行います。必要に応じて、クラウドサービスプロバイダーが提供するラベリングをサポートする機能を採用することができます。

視察の権利

サプライヤーは、Barclays による**少なくとも 10 営業日**前の書面による通知により、サプライヤーがその Barclays に対する義務へのコンプライアンスを果たしているかを審査するため、サプライヤーまたは下請業者/復処理者が役務に使用しているサプライヤーシステムの開発、テスト、改良、保全のために使用する現場または技術に対し、Barclays がセキュリティー審査を実施することを許可しなければなりません。 サプライヤーは、Barclays に年に 1 回の視察、および/またはセキュリティーインシデント後の即時の視察を許可しなければなりません。

視察中に Barclays により管理の非遵守が特定された場合、Barclays によるリスク評価が行われなければなりません。Barclays は改善期間を定める必要があります。サプライヤーは、その後、期間内に必要な改善を完了しなければなりません。

サプライヤーは、視察および視察中に提出された書類に関連して Barclays から合理的に要求されたすべてのサポートを提供する必要があります。文書は記入し、速やかに Barclays に返送する必要があります。また、サプライヤーは保証審査中に要求された証拠とともに、Barclays の評価質問者をサポートする必要があります。

付属書 A：Barclays 情報ラベリングスキーム - データ取り扱い要件

表 A1：Barclays 情報ラベリングスキーム

ラベル	定義	例
秘密	情報は、エンタープライズリスク管理枠組み（ERMF）の下で「最重要」と評価され（財務または非財務）、その不正な開示が Barclays にマイナスの影響を及ぼす場合、**秘密**として分類されるものとします。 この情報は特定の対象者に制限され、作成者の許可なしにさらに配布してはなりません。対象者には情報所有者の明示的な許可を受けた社外の受取人が含まれる場合があります。	• 吸収合併または買収可能性の情報 • 戦略的な計画情報 - ビジネスと組織 • 特定の情報セキュリティの設定に関する情報 • 特定の監査所見およびレポート • 執行委員会議事録 • 認証または本人確認および検証（ID&V）詳細 - 顧客/取引先および社員 • 大量のカードホルダー情報 • 利益予測または年度決算結果（一般公開前） • 正式な機密保持契約（NDA）で対象となっている項目
社内秘	想定されている受取人が Barclays の認証された社員であるか、Barclays と有効な契約を締結した特定の対象者に限定された Barclays マネージドサービスプロバイダー（MSP）のみである場合、情報は**社内秘**として機密情報に分類されるものとします。 エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「関係者外秘」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays に悪い影響を及ぼす場合があります。 この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 戦略および予算 • 成績評価 • スタッフの報酬および個人情報 • 脆弱性評価
社外秘	想定されている受取人が Barclays の認証された社員であるか、Barclays と有効な契約を締結した特定の対象者に限定された Barclays マネージドサービスプロバイダー（MSP）、または情報の所有者によって承認された外部の関係者のみである場合、情報は**社外秘**として機密情報に分類されるものとします。 エンタープライズリスク管理枠組み（ERMF）の下で「重要」または「限定」と評価される情報（財務または非財務）は、不正に開示された場合 Barclays にマイナスの影響を及ぼす場合があります。	• 新製品計画 • 依頼人契約書 • 法的契約書 • 外部への送信を目的とした個人・少数顧客・取引先情報 • 顧客/取引先への通信。 • 新情報を提供する新しい発行物（目論見書、募集要項など） • 最終調査報告書 • Barclays 外へ非公開の重大な情報（MNPI）

	この情報は一般的な配布を意図していませんが、知る必要の原則に従って受取人は転送または共有することができます。	• 全調査報告書 • 特定のマーケティング資料 • 市場解説 • 監査所見およびレポート
制限なし	情報は、一般配布を目的としているか、または配布されても組織に悪影響を与えない場合、「制限なし」に分類されるものとします。	• マーケティング資料 • 出版物 • 公示 • 求人広告 • Barclays に影響を及ぼさない情報

表 A2：Barclays 情報ラベリングスキーム - データ取り扱い要件

*** システムセキュリティ設定情報、監査所見、および個人情報は、無許可の開示がビジネスに及ぼす影響により、社内秘または秘密のいずれかに分類される場合があります

ライフサイクル段階	秘密	社内秘	社外秘
作成および導入	• 資産には情報所有者を割り当てることが必須。	• 資産には情報所有者を割り当てることが必須。	• 資産には情報所有者を割り当てることが必須。
保存	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。 • 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。 • Barclays のデータ、アイデンティティ、および/または名声を保護するために使用されるすべてのプライベート鍵は、FIPS 140-2 レベル 3 以上の証明書付きハードウェアセキュリティモジュール（HSM）により保護されるものとします。	• 資産（物理または電子）は、公共エリア（訪問者が監視されずにアクセスすることが可能なサプライヤー施設内の公共エリアを含む）に保管してはなりません。 • 情報は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所に保管してはなりません。 • 保管中の電子資産は、許可を受けない人物がアクセスできる重大なリスクがある場合は、暗号化または適切な補償管理によって保護することが必須です。

アクセスおよび使用	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。 資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。 • 印刷される資産は、印刷セキュリティツールを使用して印刷するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。	• 資産（物理または電子）は、施設外の公共エリアに放置してはなりません。 • 資産（物理または電子）は、訪問者が監視されることなくアクセスが可能な施設内の公共エリアに放置してはなりません。 • 電子資産は、必要に応じ、適切な論理的アクセス管理により保護するものとします。	• 資産（物理または電子）は、許可を受けない人物が表示またはアクセスできる場所で作業したり、無人状態で放置してはなりません。 資産は、適切な管理が確立されている場合のみ作業可能です（覗き見防止フィルムなど）。 • 印刷された資産は、速やかにプリンターから回収するものとします。 それが不可能な場合は、印刷セキュリティツールを使用するものとします。 • 電子資産は、適切な論理的アクセス管理により保護するものとします。
共有	• 紙印刷された資産には、全ページに明確な情報ラベルを付けるものとします。 • 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼り、開封明示シールを貼るものとします。それらは配布前に、ラベルのない別の封筒に入れるものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーのみを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、情報所有者により受信を個別に許可された人員のみに配布するものとします。 • 資産はファックスで送信してはなりません。	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーのみを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。	• 紙印刷された資産には、明確な情報ラベルを貼るものとします。 ラベルは、最低でもタイトルページに貼るものとします。 • 紙印刷された資産が入っている封筒には、表面に明確な情報ラベルを貼るものとします。 • 電子資産には、明確な情報ラベルを付けるものとします。 複数ページの電子文書のコピーには、全ページに明確な情報ラベルを付けるものとします。 • 資産は、必ず組織により承認されたシステム、方法、またはサプライヤーを使用して配布するものとします。 • 資産は、組織により雇用された、または、適切な契約上の義務がある人員宛、または、契約交渉など明確に認識されたビジネスの一貫として配布されるものとします。 • 資産は、それを受け取るためのビジネス上のニーズがある人員のみに配布するものとします。 • 資産は、受信者がその資産をすぐに回収できることを送信者が確認していない限り、ファックスで送信してはなりません。

	• 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。 • 電子資産の流通管理を維持するものとします。		• 電子資産を社内ネットワーク外に転送する場合は、承認済みの暗号保護メカニズムを使用して暗号化するものとします。
アーカイブ化と処分	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。 • 秘密電子資産が保存されていたメディアは、処分の前または処分中に、適切に機密情報を分離するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。	• 紙印刷された資産は、機密文書廃棄処理サービスを使用して処分するものとします。 • 電子資産のコピーは、システムの「ごみ箱」または類似の機能から適時削除するものとします。

付属書 B：定義

Barclays の機密情報とは、本一般利用規約、および/または過去、現在、または将来の（i）Barclays 企業の事業活動、製品および/または開発物、および/または（ii）Barclays 企業（サプライヤー企業を除く）の従業員、顧客、カウンターパーティ、第三者/サプライヤーおよび/または下請業者に関係する契約に関連して、サプライヤーリード、サプライヤーまたはサプライヤーの人員が取得する情報（またはそれらの者がアクセスできる情報）を意味します。これには、Barclays 企業が所有する知的財産（契約に基づくものを含む）または第三者のサプライヤー/請負業者が所有する知的財産、保護対象個人データ、本一般条件、各モジュールおよび各契約、契約に基づいて維持される記録、ならびに該当する企業または個人の計画、価格、方法、プロセス、財務データ、知的財産権、研究、システム、プログラム、および/または情報技術の一切が含まれます。

Barclays のデータとは、あらゆる媒体（（i）本契約に関連してサプライヤーがアクセス可能であるか、（ii）Barclays 企業によりサプライヤーに提供されるか、または（iii）サプライヤーが契約に関連して生成、収集、処理、保存、または送信する、サプライヤーの資材を除くすべての電子媒体、光学媒体、磁気媒体または有形媒体を含む）に組み込まれたすべてのデータ、情報、テキスト、図面およびその他の資料を意味します。

Barclays のシステムとは、Barclays 企業が所有、管理、運営、使用する 1 つ以上のハードウェア、機器、ソフトウェア、周辺機器および通信ネットワークで構成される電子情報システムを意味します。

サイバーインシデントとは、イベントが実際に発生したことが確認されたか、サプライヤーまたは Barclays が（信頼し得る脅威、インテリジェンスなどに基づいて）発生を信じる合理的な根拠を有するか否かを問わず、その結果として、（i）Barclays のデータの機密性、完全性または完

全可用性、あるいは（ii）サプライヤーのシステムまたは Barclays のシステムの機密性、完全性、完全可用性、および通常の運用に危険をもたらす、または危険をもたらす可能性のあるあらゆるイベントを意味します。

データ保護影響評価とは、データ保護法で要求される、個人データ保護に対する想定された処理業務の影響評価を意味します。

データ保護法とは、本契約に基づくサプライヤーの義務の履行に適用される範囲において、以下を意味します。（i）プライバシーおよび電子通信に関する EU 指令 2002/58/EC（随時修正または置換される）、（ii）EU 一般データ保護規則 2016/679（GDPR）、欧州委員会の決定および指針、およびすべての国内施行法、（iii）英国 GDPR、（iv）非公開個人情報に関するグラムリーチブライリー法の規定、（v）1996 年医療保険の携行性と責任に関する法律、（vi）（a）Barclays 企業が所在するか、サプライヤーの義務が履行されるか、関連するデータ主体が所在するか、または保護対象個人データが処理、保管もしくは使用される法域、および（b）サプライヤーが契約に基づいて義務を履行する法域における、データ保護およびプライバシーに関するその他すべての適用法、規制、規制当局の指針。

データプライバシー管理義務とは、スケジュール 7（外部サプライヤー管理義務）の一部を構成するデータプライバシースケジュールを意味します。

データ主体とは、データ保護法において定められる意味を有します。データ保護法により上記の用語が定義されていない場合は、識別された自然人または識別可能な自然人を意味します。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的同一性に特有の 1 つ以上の要因を参照することによって、直接的または間接的に識別可能な自然人のことを指します。

データ転送契約とは、（その状況に応じて）該当する英国個人データ、EU 個人データ、および/または EU 以外/英国以外の個人データがデータ保護法の規定に従って適切に保護されるようにするために、Barclays が合理的に決定した条件に基づいて定められたデータ転送契約を意味します。

業界の最良慣行とは、事業および状況に関連して、同一または類似の状況下で同種の事業に従事する高度な技能および経験を有する者に合理的に期待される最高水準の技能、勤勉さ、慎重さ、先見性を行使することを意味します。

個人データとは、データ保護法において定められる意味を有します。上記の用語がデータ保護法で定義されていない場合は、データ主体に関連する情報、またはデータ主体を直接的または間接的に識別する情報を意味します。

個人データ侵害とは、データ保護法において定められる意味を有します。上記の用語がデータ保護法で定義されていない場合は、送信、保管またはその他処理される個人データの偶発的または違法な破壊、損失、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ー違反を意味します。

処理とは、データ保護法において定められる意味を有します。　上記の用語がデータ保護法において定義されていない場合は、自動的な手段であるか否かにかかわらず、収集、記録、整理、保管、適合または変更、取得、参照、使用、送信による開示、流布またはその他の公開、整合または結合、ブロック、消去または破棄など、個人データに対して行われる操作または一連の操作を意味し、**処理する**および**処理された**はこれに準ずる意味を有するものとします。

下請業者とは、以下に関連して随時商品および/またはサービスを提供する第三者を意味します。（a）本製品、本サービスおよび/または本成果物の提供、および/または（b）契約で許可される保護対象個人データの処理またはその他の使用。

サプライヤー/第三者の人員とは、本契約に基づいて本サービスの一部を遂行するか、または本製品を提供するすべての個人または企業を意味し、これにはサプライヤーまたはその下請業者の従業員、下請業者および/または代理人が含まれます。

サプライヤー/第三者のシステムとは、以下（またはその一部）に該当する電子情報システム（1 つ以上のハードウェア、機器、ソフトウェア、周辺機器および通信ネットワークを含む場合があります）を意味します。（i）契約に関連して、Barclays 関連会社に本製品または本サービスを提供するために使用される、または（ii）契約に関連してサプライヤーまたは下請業者の保管、管理、監視または支配下にあるもの。

本システムとは、本契約に関連してあらゆる商品または本サービスを Barclays 関連会社に提供するために使用される電子情報システム（1 つ以上のハードウェア、機器、ソフトウェア、周辺機器および通信ネットワークを含む場合があります）を意味します。