

Obligations de contrôle pour les fournisseurs externes

Sécurité des informations et cybersécurité

Pour les fournisseurs classés à risque lié aux
informations et à cyber-risque élevés

Domaine/intitulé du contrôle	Description du contrôle	Raisons de l'importance
<p>1. Gouvernance, politique et normes en matière de sécurité des informations / cybersécurité</p>	<p>Le fournisseur doit mettre en place des processus de gouvernance en matière de risques liés aux informations / cyber-risques assurant la bonne compréhension de son environnement technologique et du statut des contrôles de sécurité des informations/cybersécurité, ainsi qu'un programme de sécurité destiné à protéger le fournisseur contre toute menace liée aux informations/cybermenace conformément aux bonnes pratiques du secteur (dont les publications du NIST et du SANS et la norme ISO 27001) ainsi qu'aux exigences applicables de l'industrie.</p> <p>Le fournisseur doit évaluer régulièrement les risques liés à la sécurité des informations/cybersécurité (et en aucun cas moins d'une fois par an) et mettre en œuvre les contrôles et les étapes requis pour réduire les risques identifiés. Si un risque substantiel susceptible de nuire à la réputation de Barclays ou au service qui lui est fourni est identifié, le fournisseur doit en avertir Barclays.</p> <p>Le fournisseur doit appliquer des politiques approuvées par la direction supérieure, et des normes de gestion des risques liés aux informations/cyber-risques encourus par le fournisseur, et doit réviser ces dernières au moins une fois par an.</p>	<p>En cas de non-mise en œuvre de ce contrôle, Barclays ou ses fournisseurs pourraient ne pas bénéficier d'une surveillance appropriée en matière de sécurité des informations/cybersécurité ou être dans l'incapacité d'apporter la preuve de cette surveillance.</p> <p>Des politiques et normes documentées sont des éléments primordiaux pour la gestion et la gouvernance des risques. Elles définissent la vision par la direction des contrôles nécessaires pour gérer les risques liés aux informations/cyber-risques.</p>

<p>2. Usage approuvé</p>	<p>Le fournisseur doit définir et publier des critères d'utilisation acceptable pour informer son personnel de ses responsabilités.</p> <p>Les domaines suivants doivent être pris en compte :</p> <ul style="list-style-type: none"> (a) Utilisation d'Internet ; (b) Utilisation des médias sociaux ; (c) Utilisation de la messagerie électronique d'entreprise ; (d) Utilisation de la messagerie instantanée ; (e) Utilisation du matériel informatique fourni par le fournisseur ; (f) Utilisation du matériel informatique non fourni par le fournisseur (par ex. Apportez votre équipement personnel de communication) ; (g) Utilisation de dispositifs de stockage portables/amovibles ; (h) Responsabilités lors de la gestion d'actifs informationnels Barclays ; et (i) Sortie des canaux de fuite de données <p>Le fournisseur doit prendre les mesures appropriées pour s'assurer du respect des critères d'utilisation acceptable.</p>	<p>Les critères d'utilisation acceptable aident à soutenir l'environnement de contrôle en protégeant les actifs informationnels.</p>
<p>3. Rôles et responsabilités</p>	<p>Le fournisseur doit définir et communiquer les rôles et responsabilités relatifs à la sécurité des informations/ cybersécurité. Ceux-ci doivent être révisés régulièrement (et dans tous les cas au moins une fois tous les 12 mois) et après chaque changement matériel apporté à l'activité ou au modèle d'exploitation du fournisseur.</p> <p>Parmi les rôles clés doit figurer un cadre supérieur, qui sera responsable de la sécurité des informations/cybersécurité.</p>	<p>La définition claire des rôles et des responsabilités soutient la mise en œuvre de l'annexe Obligations de contrôle pour les fournisseurs externes.</p>

<p>4. Respect des exigences légales locales</p>	<p>Le fournisseur doit s'assurer que les exigences légales liées à la sécurité des informations applicables dans la juridiction dans laquelle le fournisseur exerce ses activités sont respectées et que ce respect est documenté de manière appropriée.</p> <p>N.B. Des exigences supplémentaires peuvent être spécifiées par les équipes locales en lien avec la législation et la réglementation bancaires locales pour les fournisseurs soutenant Barclays Suisse et Barclays Monaco.</p>	<p>Le défaut de respect des exigences légales locales pourrait avoir de graves conséquences pour le fournisseur comme pour Barclays, au nombre desquelles la condamnation à des amendes et, dans des cas extrêmes, la perte par Barclays de son agrément bancaire.</p>
<p>5. Formation et sensibilisation</p>	<p>Le fournisseur doit dispenser une formation et une sensibilisation (F&S) auprès de l'ensemble des employés concernés. Cette F&S doit être adaptée à leurs rôles et responsabilités et doit être suffisante pour que les employés soient à même de comprendre et d'identifier des événements susceptibles de constituer des attaques et de signaler leurs préoccupations. Au minimum, la formation doit porter sur la protection de sa sécurité en ligne (au bureau, chez soi et lors de déplacements), les risques liés à l'ingénierie sociale et les contre-mesures pratiques.</p> <p>Le fournisseur doit s'assurer que l'ensemble des membres du personnel (nouvelles recrues/employés mutés), dans un délai raisonnable, suivent la formation pour s'assurer qu'ils comprennent leurs rôles et responsabilités liés à la sécurité des informations.</p> <p>Une formation de sensibilisation au renforcement de la sécurité des informations/cybersécurité doit être dispensée aux administrateurs systèmes au moins une fois par an pour leur communiquer des informations sur les scénarios/menaces spécifiques à leur rôle et la manière d'identifier les menaces liées aux informations/cybermenaces, de se protéger contre les menaces liées aux informations/cybermenaces et de signaler des préoccupations.</p>	<p>La formation et la sensibilisation viennent à l'appui de tous les autres contrôles présentés dans cette annexe.</p> <p>En cas de non-mise en œuvre de ce contrôle, les employés pertinents ne seront pas informés des cyber-risques et des vecteurs utilisés pour mettre en œuvre des attaques et seront dans l'incapacité de détecter ou de prévenir des attaques.</p>

<p>6. Processus de gestion des incidents</p>	<p>Un processus de réponse en cas d'incident destiné à gérer en temps opportun et à signaler régulièrement les incidents impliquant des informations de Barclays et/ou des services utilisés par Barclays doit être défini et géré. Ce qui suit doit être défini dans le cadre de la procédure de réponse en cas d'incident :</p> <ul style="list-style-type: none"> • Les incidents de sécurité et les violations des données ayant affecté et/ou visé des actifs de Barclays et/ou des services fournis à Barclays doivent être signalés à Barclays dans les meilleurs délais et Barclays doit être tenue informée de l'état d'avancement des mesures correctives mises en œuvre. • Un processus de réponse en cas d'incident destiné à gérer en temps opportun et à signaler régulièrement les intrusions impliquant des informations de Barclays et/ou des services utilisés par Barclays doit être défini. • Les violations qui ne semblent pas avoir affecté le système de Barclays ainsi que les mises à jour/mesures correctives mises en œuvre doivent également être signalées à Barclays, à des fins d'information. • Le fournisseur doit s'assurer que les équipes de réponse en cas d'incident et les processus pertinents en cas d'incident sont contrôlés au moins une fois par an pour s'assurer de la capacité du fournisseur à répondre à des incidents liés à la cybersécurité identifiés. Le contrôle doit inclure la confirmation de la capacité à informer Barclays, dont la preuve sera apportée en démontrant la capacité à contacter les personnes appropriées. • Un processus doit être défini et exploité pour identifier et gérer l'atténuation des vulnérabilités après un incident de sécurité sans compromettre les investigations ni les activités de réponse. • Le fournisseur doit disposer de processus et de procédures pour effectuer une analyse des causes profondes des événements internes (au fournisseur) et externes. • Le fournisseur doit s'assurer que les mesures correctives identifiées à la suite d'un incident sont traitées selon un plan correctif (action, propriété, date de livraison), et partagées et approuvées par Barclays. 	<p>L'existence d'un processus de gestion et de réponse en cas d'incident aide à assurer la maîtrise rapide et à éviter l'aggravation des incidents.</p>
--	--	---

7. Amélioration continue	Le fournisseur doit, de manière continue, tirer des enseignements des événements et mettre ces enseignements en pratique pour améliorer ses moyens de défense contre les cyber-risques.	En cas de non-mise en œuvre de ce contrôle, les fournisseurs seront dans l'incapacité d'utiliser les enseignements tirés d'événements antérieurs pour améliorer et renforcer leur environnement de contrôle.
8. Propriété des actifs informationnels	Le fournisseur doit disposer d'un contact désigné pour communiquer avec le propriétaire d'un actif informationnel de Barclays.	La propriété des actifs informationnels est fondamentale pour assurer la protection adaptée des actifs informationnels.
9. Schéma d'étiquetage des informations	<p>Le cas échéant*, le fournisseur doit appliquer le schéma d'étiquetage des informations Barclays et les exigences de gestion (Annexe B, Tableau B1 et B2A2), ou un autre programme convenu avec Barclays, à l'ensemble des actifs informationnels détenus ou traités pour le compte de Barclays.</p> <p><i>* « le cas échéant » fait référence à l'avantage qu'apporte l'étiquetage par rapport au coût associé. Par exemple, l'étiquetage d'un document n'est pas approprié si cela conduit à la violation des exigences anti-violation réglementaires.</i></p>	L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés.
10. Gestion des actifs	Le fournisseur doit tenir un inventaire précis de tous les actifs informatiques appropriés utilisés pour fournir des services à Barclays et doit le réviser au moins une fois par an pour s'assurer qu'il est à jour, complet et exact.	En cas de non-mise en œuvre de ce contrôle, les actifs de Barclays ou les actifs utilisés par les fournisseurs pour fournir des services à Barclays pourraient être compromis, ce qui pourrait se traduire par des pertes financières, des pertes de données, une atteinte à la réputation et des sanctions réglementaires.

11. Sécurité en cours de transit	Les actifs informationnels Barclays (sauf s'ils sont considérés comme des actifs « Sans aucune restriction » ou équivalents) doivent être protégés en cours de transit proportionnellement au risque associé.	Les contrôles applicables en cours de transit protègent les informations de Barclays contre toute interception et toute divulgation.
12. Destruction/suppression/déclassement d'informations physiques et logiques	Les actifs informationnels Barclays stockés sous format physique ou électronique, doivent être détruits ou supprimés de manière sécurisée en fonction de leur risque associé, en s'assurant qu'ils ne sont pas récupérables.	La destruction sécurisée des actifs informationnels aide à s'assurer que les actifs informationnels Barclays ne peuvent pas être récupérés pour toute violation de données ou perte ou activité malveillante.

<p>13. Sécurité du réseau</p>	<p>Le fournisseur doit s'assurer que l'ensemble des systèmes informatiques exploités par le fournisseur ou son sous-traitant qui soutiennent des services fournis à Barclays sont protégés contre un mouvement latéral de menaces au sein du réseau du fournisseur (et de tout sous-traitant concerné).</p> <p>Les mécanismes de protection suivants doivent être pris en compte par le fournisseur :</p> <ul style="list-style-type: none"> • au moyen d'une séparation logique des ports/interfaces de gestion des appareils du trafic utilisateurs ; • contrôles d'authentification appropriés ; et • activation de tous les contrôles d'atténuation d'exploitation disponibles au sein du système d'exploitation et des applications et agents installés. <p>Les capacités doivent être définies et exploitées par le fournisseur pour détecter les appareils non autorisés, les logiciels identifiés comme étant malveillants et les logiciels non autorisés à haut risque sur le réseau du fournisseur.</p> <p>Des capteurs de réseau doivent être positionnés par le fournisseur pour détecter les menaces à tous les points d'entrée et de sortie du périmètre du réseau.</p> <p><i>N.B. Le terme « réseau » tel qu'employé dans le présent contrôle désigne tout réseau qui n'est pas un réseau Barclays, dont le fournisseur est responsable, y compris le réseau du sous-traitant du fournisseur.</i></p>	<p>En cas de non-mise en œuvre de ce contrôle, les réseaux externes et internes pourraient être compromis par des auteurs de menace.</p>
<p>14. Protection du périmètre</p>	<p>Le fournisseur doit tenir à jour un inventaire des connexions à un réseau externe, des systèmes hôtes accessibles par Internet et des transferts de données utilisés pour retourner des données à Barclays ou à des tiers (y compris, de façon non limitative, à des sous-traitants du fournisseur).</p> <p>Un réseau séparé plurizone doit être mis en œuvre dans le périmètre en fonction de l'exposition aux risques et des besoins commerciaux.</p> <p>Le périmètre doit uniquement comprendre les appareils qui doivent nécessairement disposer d'un accès entrant ou sortant à des réseaux externes ou qui facilitent cet accès.</p>	<p>La protection appropriée du périmètre aide à assurer la protection appropriée du réseau et des actifs informationnels de Barclays.</p>

<p>15. Accès au réseau et accès à distance</p>	<p>Le fournisseur doit s'assurer que l'accès au réseau interne est surveillé et que seuls les appareils autorisés sont acceptés au moyen des contrôles d'accès au réseau appropriés.</p> <p>Lorsque l'accès à distance aux actifs informationnels Barclays stockés au sein de l'environnement géré par le fournisseur est accepté, des mécanismes d'authentification et d'autorisation à deux facteurs du point d'extrémité doivent être en place, lesquels doivent tenir compte de l'identité de l'utilisateur, du type d'appareil et du degré de sécurité présenté par l'appareil (par exemple, niveau des correctifs, état des mécanismes de protection contre les logiciels malveillants, appareil mobile permettant ou non l'exercice de droits d'utilisateur privilégiés, etc.).</p> <p>L'accès à distance aux environnements Barclays n'est pas assuré par défaut pour une connexion depuis le site du fournisseur/pour toute assistance en cas d'absence du bureau ou en dehors des heures de travail. Tout accès à distance doit être approuvé par les équipes Barclays concernées (y compris le Responsable de la sécurité).</p>	<p>Les contrôles d'accès au réseau aident à assurer l'absence de connexion au réseau du fournisseur d'appareils non sécurisés qui pourraient introduire de nouvelles vulnérabilités.</p>
<p>16. Détection des dénis de service</p>	<p>Le fournisseur doit mettre en œuvre et préserver des capacités de détection des attaques par déni de service (DdS).</p> <p>Le fournisseur doit s'assurer que les canaux connectés à Internet ou externes soutenant les services fournis à Barclays disposent d'une protection DdS adéquate pour garantir les critères de disponibilité convenus avec Barclays.</p>	<p>En cas de non-mise en œuvre de ce contrôle, Barclays et ses fournisseurs pourraient être dans l'incapacité d'empêcher une attaque par déni de service d'atteindre l'objectif visé par son auteur.</p>

<p>17. Surveillance/consignation d'informations</p>	<p>Le fournisseur doit s'assurer qu'une capacité de surveillance 24 h/24, 7 j/7 de l'infrastructure informatique en vue d'identifier d'éventuels événements en matière de cybersécurité est en place.</p> <p>Le fournisseur doit collecter et corréler les données relatives aux événements à partir des capteurs et des sources du système pertinents et les analyser en vue d'identifier et comprendre les attaques/incidents. Lors de l'identification d'un incident matériel et/ou d'une violation des contrôles de sécurité, le fournisseur doit s'assurer du suivi du processus de gestion des incidents (à la section 6 ci-dessus).</p> <p>Tous les systèmes clés, y compris les applications clés, doivent être configurés par le fournisseur pour consigner les événements clés dans un journal et l'heure système des différents systèmes doit être synchronisée par le fournisseur via le protocole horaire en réseau (NTP).</p> <p>Les journaux doivent être centralisés, sécurisés de manière appropriée et conservés par le fournisseur pour une durée minimale de 12 mois.</p> <p>Les événements clés consignés dans un journal doivent comprendre les événements susceptibles d'avoir une incidence sur la confidentialité, l'intégrité et la disponibilité du service fourni à Barclays, et qui peuvent faciliter l'identification ou la recherche d'incidents matériels et/ou de violations des droits d'accès liés aux systèmes du fournisseur.</p>	<p>En cas de non-mise en œuvre de ce contrôle, les fournisseurs seront dans l'incapacité de détecter des atteintes à la cybersécurité et d'y répondre, ou d'assurer le rétablissement et d'analyser les journaux pertinents en vue de tirer des enseignements des événements informatiques survenus sur leur réseau.</p>
<p>18. Séparation des actifs informationnels</p>	<p>Le fournisseur doit stocker les actifs informationnels Barclays dans un réseau séparé (logiquement et/ou physiquement) des autres clients.</p>	<p>L'existence d'un réseau séparé aide à assurer la protection appropriée des actifs informationnels de Barclays contre toute divulgation non autorisée.</p>

<p>19. Protection contre les logiciels et codes malveillants</p>	<p>Lorsqu'ils sont supportés au niveau du système d'exploitation, les systèmes informatiques, services informatiques et appareils informatiques doivent être dotés d'une solution contre les logiciels malveillants à tous moments afin de prévenir les perturbations de service ou les violations de sécurité.</p> <p>Le fournisseur doit :</p> <ul style="list-style-type: none"> • établir et maintenir une protection à jour contre les logiciels et codes malveillants, conformément aux bonnes pratiques du secteur (par ex. les publications du NIST et la norme ISO 27001) ; et • protéger les systèmes de Barclays, de ses clients et d'autres tiers contre tout transfert de codes malveillants conformément aux méthodes normalisées du secteur (par ex. les publications du NIST et la norme ISO 27001). 	<p>Les solutions contre les logiciels malveillants sont cruciales pour la protection des actifs informationnels Barclays contre les codes malveillants.</p>
<p>20. Normes applicables aux infrastructures sécurisées et rapprochement des changements en matière de sécurité</p>	<p>Le fournisseur doit définir des normes applicables aux infrastructures pour tous les logiciels prêts à l'emploi configurables utilisés en grand nombre (par exemple les systèmes d'exploitation et les bases de données) et le matériel des infrastructures d'utilisation courante (par exemple les appareils SAN ou les appareils du réseau). Tout défaut de respect des normes applicables aux infrastructures doit être corrigé. Les changements en matière de sécurité (par exemple les changements apportés à la configuration des mécanismes de sécurité, la modification des privilèges accordés à un compte) doivent toujours donner lieu à la création d'un élément de journal consigné dans un environnement infalsifiable. Un rapprochement doit être opéré entre les changements effectués et les changements autorisés.</p> <p>Les systèmes hôtes et les appareils reliés au réseau inclus dans les systèmes du fournisseur doivent être configurés pour fonctionner en conformité avec les bonnes pratiques du secteur (par exemple, les publications du NIST et du SANS et la norme ISO 27001).</p>	<p>Les contrôles relatifs aux normes applicables aux infrastructures aident à protéger les actifs informationnels contre tout accès non autorisé.</p> <p>Le respect des normes applicables aux infrastructures et les contrôles permettant de s'assurer que les changements sont autorisés aident à assurer la protection des actifs informationnels de Barclays.</p>
<p>21. Technologies de protection de la sécurité</p>	<p>Les technologies appropriées doivent être appliquées pour traiter les cybermenaces effectives et émergentes et des contrôles de base réalisés en permanence pour prévenir tout lancement, toute exécution et toute exploitation d'une attaque et toute exfiltration.</p>	<p>En cas de non-mise en œuvre de ce contrôle, les actifs informationnels de Barclays pourraient ne pas être suffisamment protégés contre les cyberattaques.</p>

<p>22. Sécurité des points d'extrémité</p>	<p>Le fournisseur doit s'assurer que les points d'extrémité utilisés pour accéder au réseau de Barclays ou pour traiter des données de Barclays sont renforcés à des fins de protection contre les attaques.</p> <p>Ces mesures incluent, de façon non limitative, le fait de limiter la portée des attaques en désactivant les logiciels/services/ports non nécessaires et de s'assurer que toutes les versions déployées sont suffisamment récentes pour bénéficier de l'assistance au public, que tous les mécanismes de protection contre les logiciels malveillants et de pare-feu des systèmes hôtes ont été mis en place et correctement configurés et que des mesures de contrôle destinées à limiter les tentatives d'exploitation ont été mises en place.</p>	<p>En cas de non-mise en œuvre de ce contrôle, le réseau et les points d'extrémité de Barclays et du fournisseur pourraient être vulnérables aux cyberattaques.</p>
<p>23. Détection des appareils et des logiciels non autorisés</p>	<p>Le fournisseur doit s'assurer qu'il dispose des capacités et a mis en place les processus nécessaires pour détecter les appareils non autorisés, les logiciels identifiés comme des logiciels malveillants et les logiciels non autorisés à haut risque.</p>	<p>En cas de non-mise en œuvre de ce contrôle, les fournisseurs pourraient être dans l'incapacité de détecter, supprimer ou désactiver des appareils ou logiciels non autorisés et malveillants, ce qui exposerait les actifs de Barclays à des cyberattaques.</p>
<p>24. Prévention des fuites de données</p>	<p>Le risque de fuite de données concernant les informations se rapportant au(x) service(s) que le fournisseur fournit à Barclays découlant du réseau ou du support physique doit être évalué et atténué.</p> <p>Les canaux de fuite de données suivants doivent être pris en compte :</p> <ul style="list-style-type: none"> • transfert non autorisé d'informations à l'extérieur du réseau interne / réseau du fournisseur. • perte ou vol d'actifs informationnels Barclays sur des supports électroniques portables (y compris informations électroniques sur des ordinateurs portables, appareils mobiles, et supports portables) ; • transfert non autorisé d'informations vers des supports portables ; • échange d'informations non sécurisé avec des tiers (sous-traitants) ; • impression ou copie inappropriée d'informations ; • erreurs et omissions au niveau de la classification et de l'étiquetage des actifs ; et • fuite non autorisée d'informations via le système de noms de domaines (SND) 	<p>Les contrôles de prévention des fuites de données appropriés constituent un élément crucial de la sécurité des informations, en ce qu'ils contribuent à assurer l'absence de pertes d'informations Barclays.</p>

25. Stockage et traitement sécurisés	Des contrôles doivent être mis en place pour assurer la protection des actifs informationnels (se rapportant au(x) service(s) que le fournisseur fournit à Barclays) indépendamment de l'endroit où ils sont stockés ou traités (ce qui précède s'appliquant aux informations stockées conformément aux méthodes structurées et non structurées).	Les actifs informationnels sont généralement stockés ensemble et, à ce titre, ils représentent une concentration de risques et doivent faire l'objet d'une sécurisation.
26. Sauvegardes et récupération	<p>Des dispositions doivent être prises pour s'assurer que les informations sont dûment sauvegardées et récupérables conformément aux exigences convenues avec le Propriétaire des actifs informationnels Barclays et que la sécurité des actifs informationnels est préservée tout au long du processus.</p> <p>La fréquence et la méthode de réalisation des sauvegardes doivent être convenues avec le propriétaire des actifs informationnels.</p> <p>Les actifs informationnels sauvegardés doivent se voir appliquer des contrôles définis pour s'assurer que l'accès n'est accordé qu'en cas de besoin.</p>	Les sauvegardes comprennent des copies d'actifs informationnels et, à ce titre, elles doivent être soumises aux mêmes contrôles.

<p>27. Gestion de l'accès logique (LAM)</p>	<p>L'accès aux informations doit être soumis à restrictions, et en prenant dûment en considération les principes du besoin de connaître, du moindre privilège et de séparation des tâches. Le propriétaire des actifs informationnels est chargé de décider des personnes qui doivent accéder et de leur niveau d'accès.</p> <ul style="list-style-type: none"> • Le principe du besoin de connaître veut que les personnes aient seulement accès aux informations qu'elles ont besoin de connaître afin d'exécuter leurs tâches autorisées. Par exemple, si un employé traite exclusivement avec des clients basés au Royaume-Uni, il n'a pas « besoin de connaître » des informations se rapportant aux clients basés aux États-Unis. • Le principe du moindre privilège veut que les personnes bénéficient seulement du niveau minimum de privilège nécessaire pour exécuter leurs tâches autorisées. Par exemple, si un employé a besoin de voir l'adresse d'un client mais ne sera pas tenu de la modifier, le « moindre privilège » dont il doit bénéficier est alors un accès en lecture seule, qui doit lui être accordé à la place d'un accès lecture/écriture. • Le principe de séparation des tâches veut qu'au moins deux personnes soient responsables de parties séparées de toute tâche afin de prévenir toute erreur et toute fraude. Par exemple, un employé qui demande la création d'un compte ne doit pas être celui qui approuve la demande. <p>Ces principes doivent être appliqués en fonction des risques, en prenant en compte le niveau de confidentialité des informations.</p> <p>Chaque compte doit être associé à une seule personne, qui sera responsable de toute activité conduite en utilisant ce compte.</p> <p>Cela n'empêche pas l'utilisation de comptes partagés, mais une seule personne doit quand même être responsable de chaque compte partagé.</p> <p>Les processus de gestion de l'accès doivent être définis conformément aux bonnes pratiques de l'industrie et inclure, au minimum, les éléments ci-après :</p> <ul style="list-style-type: none"> • processus d'autorisation robuste en place avant la création/modification/suppression de comptes ; 	<p>L'existence de contrôles de la gestion de l'accès logique appropriés aide à assurer la protection des actifs informationnels contre toute utilisation inappropriée.</p>
---	---	--

	<ul style="list-style-type: none"> • processus d'examen périodique de l'accès des utilisateurs et au moins une fois par an pour valider l'accès des utilisateurs • contrôles des employés mutés – accès modifié/supprimé dans les 5 jours ouvrables suivant la date de mutation; • contrôles des employés quittant la société – ensemble de l'accès logique utilisé pour fournir des services à Barclays supprimé dans les 24 heures suivant la date de départ, tout autre accès secondaire supprimé dans les 7 jours ; et • les comptes inactifs non utilisés depuis 60 jours consécutifs ou plus doivent être suspendus. 	
<p>28. Méthodes d'accès</p>	<p>L'activité conduite en utilisant un compte doit pouvoir être rattachée à une personne unique. Des mesures techniques et de processus doivent être appliquées pour faire respecter le niveau approprié d'accès à l'actif informationnel.</p> <p>Les contrôles de sécurité se rapportant aux comptes (par ex. solides processus d'authentification ou de « bris de glace ») doivent être proportionnels au risque de compromission ou d'usage abusif des comptes.</p> <p>La méthode d'accès doit être définie conformément aux bonnes pratiques de l'industrie et inclure, au minimum, les éléments ci-après :-</p> <ul style="list-style-type: none"> • Les mots de passe des comptes interactifs doivent être changés au moins tous les 90 jours, et doivent être différents des douze (12) mots de passe utilisés précédemment. • Les comptes privilégiés doivent être modifiés après chaque utilisation, et au moins tous les 90 jours. • Les comptes interactifs doivent être désactivés après un maximum de cinq (5) tentatives d'accès infructueuses consécutives. <p>L'accès à distance pour les services Barclays doit être autorisé par le biais de mécanismes acceptés par les équipes Barclays concernées et doit utiliser une authentification multifacteur.</p>	<p>Les contrôles de la gestion de l'accès aident à s'assurer que seuls les utilisateurs approuvés peuvent accéder aux actifs informationnels.</p>

<p>29. Protection des applications</p>	<p>Les applications doivent être développées en utilisant des pratiques de codage sécurisées et au sein d'environnements sécurisés. Lorsque le fournisseur développe des applications destinées à être utilisées par Barclays, ou qui sont utilisées à l'appui du service fourni à Barclays, il doit mettre en place des processus et des contrôles permettant d'identifier et de corriger les vulnérabilités que pourrait comporter le code au cours du processus de développement.</p> <p>Les fichiers binaires des applications déployées et enregistrées dans les bibliothèques sources doivent être protégés contre tout changement non autorisé.</p> <p>Le fournisseur doit assurer la séparation des tâches de développement des systèmes, en s'assurant que les développeurs système n'ont pas accès à l'environnement en ligne, sauf en cas d'urgence, à condition qu'un tel accès soit protégé par des contrôles adéquats tels que des procédures « bris de glace ». De telles activités dans ces circonstances doivent être consignées et contrôlées de manière indépendante.</p>	<p>Les contrôles protégeant le développement d'applications aident à s'assurer que les applications sont sécurisées au moment du déploiement.</p>
--	--	---

<p>30. Gestion des vulnérabilités</p>	<p>Le fournisseur doit utiliser un mécanisme cohérent pour enregistrer, trier, et répondre aux vulnérabilités identifiées.</p> <p>Le fournisseur doit mettre sur pied des capacités pour identifier et classer les vulnérabilités de sécurité au sein des systèmes informatiques et des logiciels en fonction du risque sur l'ensemble des plates-formes utilisées par l'entreprise.</p> <p>Le fournisseur doit s'assurer que ses activités de référence incluent la gestion des vulnérabilités, celle-ci englobant la mise en œuvre de processus visant à détecter et évaluer le risque de vulnérabilités, à éliminer ou corriger les vulnérabilités dans tous les systèmes, et à prévenir l'introduction de nouvelles vulnérabilités lors de la mise en œuvre de processus de changement et de déploiements d'un nouveau système.</p> <p>L'ensemble des problèmes de sécurité et des vulnérabilités, susceptibles d'avoir un impact substantiel sur les systèmes de Barclays ou sur les services que le fournisseur fournit à Barclays, dont le fournisseur a décidé d'accepter le risque, doivent être communiqués à Barclays dans les plus brefs délais et convenus par écrit avec Barclays.</p> <p>Les correctifs de sécurité et les mises à jour des vulnérabilités de la sécurité doivent être installés par le fournisseur dès qu'ils sont disponibles, conformément à un processus interne approuvé (du fournisseur), pour prévenir les violations de la sécurité. Des mesures doivent être prévues pour les systèmes du fournisseur qui, pour une raison quelconque, ne peuvent être mis à jour, afin de protéger correctement les systèmes vulnérables.</p>	<p>En cas de non-mise en œuvre de ce contrôle, des pirates informatiques pourraient exploiter ces vulnérabilités des systèmes pour mener des cyber-attaques contre Barclays et ses fournisseurs.</p>
---------------------------------------	--	--

<p>31. Simulation de menaces / tests de pénétration / évaluation de la sécurité informatique</p>	<p>Le fournisseur doit faire appel à un prestataire de services de sécurité qualifié indépendant pour réaliser une évaluation de la sécurité informatique/simulation de menaces portant sur l'infrastructure et les applications informatiques se rapportant au(x) service(s) que le fournisseur fournit à Barclays.</p> <p>Cet essai ou cette évaluation doit avoir lieu au moins une fois par an afin d'identifier les vulnérabilités susceptibles d'être exploitées pour violer la confidentialité des données de Barclays par le biais de cyberattaques. Toutes les vulnérabilités doivent être hiérarchisées et suivies jusqu'à leur résolution. Tous les problèmes représentant un risque accepté doivent être communiqués à Barclays et approuvés par Barclays.</p> <p>Le fournisseur doit informer Barclays de la portée de l'évaluation de sécurité et s'accorder avec Barclays sur cette portée, en particulier sur les dates de début et de fin de l'évaluation, afin de prévenir toute perturbation des activités clés de Barclays.</p>	<p>En cas de non-mise en œuvre de ce contrôle, les fournisseurs pourraient être dans l'incapacité d'évaluer les cybermenaces auxquelles il sont confrontés et la pertinence et la solidité de leurs moyens de défense.</p>
--	---	--

<p>32. Gestion des changements et des correctifs</p>	<p>Les données de Barclays et les systèmes utilisés pour le stockage ou le traitement de telles données doivent être protégés contre toute modification inappropriée susceptible de compromettre la disponibilité ou l'intégrité.</p> <p>Le fournisseur doit développer et mettre en place une stratégie de gestion des correctifs s'appuyant sur des contrôles de gestion, des procédures de gestion des correctifs et des documents d'exploitation.</p> <p>Les correctifs de sécurité et les mises à jour des vulnérabilités de la sécurité doivent être installés dès qu'ils sont disponibles, conformément à un processus approuvé, pour prévenir les violations de la sécurité. Des mesures de sécurité doivent être appliquées pour les systèmes du fournisseur qui, pour une raison quelconque, ne peuvent être mis à jour, afin de protéger correctement les systèmes vulnérables. Toutes les modifications doivent être apportées conformément au processus de gestion des changements approuvé du fournisseur.</p> <p>La présence de vulnérabilités non résolues au niveau des applications libres doit être recherchée.</p> <p>Le fournisseur doit s'assurer que les correctifs d'urgence sont appliqués dès qu'ils sont disponibles et approuvés, sauf si cela accroît les risques pour l'entreprise. Des mesures de sécurité doivent être appliquées pour les systèmes du fournisseur qui, pour une raison quelconque, ne peuvent être mis à jour, afin de protéger correctement les systèmes vulnérables. Toutes les modifications doivent être apportées conformément au processus de gestion des changements du fournisseur.</p>	<p>La non-mise en œuvre de ce contrôle peut se traduire par la fragilisation des services face aux problèmes de sécurité, entraînant ainsi un risque de compromission des données des consommateurs, de perte de service ou d'autres activités malveillantes.</p>
<p>33. Cryptographie</p>	<p>Le fournisseur doit réviser et évaluer la technologie cryptographique et les algorithmes de chiffrement qu'il utilise afin de s'assurer que ceux-ci sont toujours adaptés aux fins poursuivies. La puissance du chiffrement déployé doit être proportionnelle à l'appétence au risque, dès lors que celle-ci pourrait avoir un impact sur les activités et les performances.</p> <p>Les mises en œuvre cryptographiques doivent respecter les exigences et les algorithmes définis.</p>	<p>L'existence d'une protection par chiffrement et d'algorithmes à jour et adaptés assure la protection ininterrompue des actifs informationnels de Barclays.</p>

34. Cloud Computing	Toute utilisation d'un service de cloud computing (public/privé/communautaire/hybride) par exemple SaaS/PaaS/IaaS dans le cadre de la prestation des services convenus à Barclays doit être examinée et approuvée par les équipes Barclays concernées (y compris le Responsable de la sécurité) ; et les contrôles permettant de protéger les informations de Barclays et le service doivent être proportionnels au profil de risque et à la criticité des actifs informationnels, afin de prévenir toute fuite de données et toute violation de la cybersécurité.	En cas de non-respect de ce principe, les actifs informationnels de Barclays incorrectement protégés pourraient être compromis, ce qui pourrait se traduire par une sanction légale ou réglementaire, ou une atteinte à la réputation de Barclays.
35. Droit d'inspection	<p>Le fournisseur, à réception d'une notification écrite de Barclays adressée au moins dix jours ouvrables à l'avance, doit autoriser Barclays à procéder à un examen de la sécurité de tout site ou toute technologie utilisé(e) par le fournisseur ou ses sous-traitants pour développer, tester, améliorer, entretenir ou exploiter les systèmes du fournisseur utilisés dans le cadre des services, afin de s'assurer que le fournisseur respecte ses obligations. Le fournisseur doit également autoriser Barclays à procéder à une inspection juste après un incident de sécurité.</p> <p>Si, au cours d'une inspection, Barclays identifie un défaut de conformité concernant les contrôles, elle effectue une évaluation des risques et précise un délai de correction. Le fournisseur prend alors toutes les mesures correctives requises avant l'expiration de ce délai. Le fournisseur doit apporter toute aide raisonnablement demandée par Barclays pour mener à bien l'inspection.</p>	Si cela n'est pas convenu, les fournisseurs seront dans l'incapacité de présenter toutes les garanties de respect de ces obligations de sécurité.
36. Espace bancaire dédié	Pour les services fournis nécessitant un espace bancaire dédié officiel, les exigences techniques et physiques d'un tel espace doivent être définies. (Si un espace bancaire dédié est requis pour le service, les exigences de contrôle à l'Annexe C s'appliqueront.)	La non-mise en œuvre de ce contrôle peut se traduire par l'absence de contrôles physiques et techniques appropriés, et donc par des retards ou des interruptions des services, ou par des violations de la cybersécurité.

Annexe A : Glossaire

Définitions	
Actif informationnel	Toute information caractérisée par une certaine valeur en termes de confidentialité, d'intégrité et de disponibilité. ou Une information ou un groupe d'informations qui présente une valeur pour l'organisation.
Authentification multifacteur	Une authentification utilisant deux techniques d'authentification différentes ou plus. Parmi les exemples figure l'utilisation d'un jeton de sécurité, où une authentification fructueuse dépend de quelque chose que la personne détient (à savoir, le jeton de sécurité) et de quelque chose que l'utilisateur connaît (à savoir, le code confidentiel du jeton de sécurité).
Chiffrement	La transformation d'un message (données, audio ou vidéo) sous une forme dénuée de sens qui ne peut pas être comprise par les lecteurs non autorisés. Cette transformation change le format texte clair en un format texte chiffré.
Code malveillant	Un logiciel écrit dans l'intention de contourner la politique de sécurité d'un système informatique, d'un appareil ou d'une application. Les virus informatiques, les chevaux de Troie et les vers informatiques en sont des exemples.
Compte	Informations d'identification (par exemple, un identifiant utilisateur et un mot de passe) par le biais desquelles l'accès à un système informatique est géré via des contrôles d'accès logique.
Compte partagé	Un compte attribué à plusieurs employés, consultants, sous-traitants ou travailleurs intérimaires disposant d'un accès autorisé et qui est utilisé lorsqu'il n'est pas envisageable de fournir des comptes individuels en raison de la nature du système auquel il est accédé.
Compte privilégié	Un compte qui dispose d'un niveau élevé de contrôle d'un système informatique donné. Un tel compte est généralement utilisé pour la maintenance des systèmes, la gestion de la sécurité ou les modifications de configuration d'un système informatique. Exemples : comptes « Administrateur », « racine », Unix avec uid=0, comptes de support, comptes de gestion de la sécurité, comptes d'administration des systèmes et comptes administrateur locaux
Cryptographie	L'application d'une théorie mathématique pour développer des techniques et algorithmes pouvant être appliqués aux données pour garantir des objectifs comme la confidentialité, l'intégrité des données et/ou l'authentification.
Déni de service (attaque par)	Une tentative de rendre une ressource informatique indisponible pour ses utilisateurs prévus.
Destruction / suppression	L'action d'écraser, d'effacer ou de détruire physiquement des informations afin qu'elles ne puissent pas être récupérées.
Espace bancaire dédié	Espace bancaire dédié désigne tous locaux qu'un membre du groupe du fournisseur ou que tout sous-traitant détient ou contrôle, qui sont exclusivement dédiés à Barclays et depuis lesquels les services sont exécutés ou fournis.

Moindre privilège	Le niveau d'accès/de permission minimal permettant à un utilisateur ou à un compte d'accomplir les fonctions professionnelles relevant de son rôle.
Propriétaire de l'actif informationnel	La personne physique, au sein de l'entreprise, chargée de classer un actif et de s'assurer de sa gestion correcte.
Sauvegarde	Une sauvegarde ou le processus de sauvegarde désigne la réalisation de copies de données afin que ces copies supplémentaires puissent être utilisées pour restaurer les données d'origine après une perte de données.
Système	Dans le cadre du présent document, un système se compose de personnes physiques, de procédures, d'équipements informatiques et de logiciels. Les éléments de cette entité complexe sont utilisés en combinaison dans l'environnement opérationnel ou d'assistance visé pour exécuter une tâche donnée ou atteindre un objectif spécifique, fournir une assistance ou satisfaire les exigences d'une mission.
Utilisateur	Un compte attribué à un employé, consultant, sous-traitant ou travailleur intérimaire du fournisseur qui dispose d'un accès autorisé à un système sans privilèges étendus.

Annexe B : Schéma d'étiquetage des informations Barclays

Tableau B1 : Schéma d'étiquetage des informations Barclays

Étiquette	Définition	Exemples
Secrètes	<p>Les informations doivent être classées « secrètes » si leur divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de la structure de gestion des risques d'entreprise (ERMF) comme étant « critique » (financier ou non-financier).</p> <p>Ces informations sont réservées à un public spécifique et ne doivent pas être diffusées ultérieurement sans l'autorisation de l'auteur. Le public peut comprendre des destinataires externes avec l'autorisation explicite du propriétaire des informations.</p>	<ul style="list-style-type: none"> • Informations sur les fusions ou acquisitions potentielles. • Informations sur la planification stratégique – commerciale et organisationnelle. • Certaines informations relatives à la configuration de la sécurité • Certains rapports et résultats d'audit. • Comptes rendus du comité exécutif. • Coordonnées d'authentification ou d'identification et de vérification (ID&V) – client et collaborateur. • Grandes quantités d'informations sur les titulaires de cartes. • Prévisions de bénéfices ou résultats financiers annuels (avant publication officielle). • Tout élément couvert en vertu d'un accord de non-divulgation (AND) formel.

Restreintes - internes	<p>Les informations doivent être classées « restreintes - internes » si les destinataires prévus sont uniquement des employés authentifiés Barclays et des prestataires de services gérés (PSG) Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique.</p> <p>Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non-financier).</p> <p>Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.</p>	<ul style="list-style-type: none"> • Stratégies et budgets. • Évaluations des performances. • Rémunération du personnel et données personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.
Restreintes - externes	<p>Les informations doivent être classées « restreintes - externes » si les destinataires prévus sont des employés authentifiés Barclays et des PSG Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique ou à des parties externes qui sont autorisées par le propriétaire des informations.</p> <p>Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non-financier).</p> <p>Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.</p>	<ul style="list-style-type: none"> • Plans de nouveaux produits. • Contrats de clients. • Contrats juridiques. • Informations clients individuelles/de petit volume destinées à être envoyées au niveau externe. • Communications avec les clients. • Documentation d'offre de nouvelle émission (par ex. prospectus, notice d'offre). • Documents de recherche finaux. • Informations importantes n'ayant pas été rendues publiques (IIPP) n'appartenant pas à Barclays. • Tous les rapports de recherche • Certains documents de marketing. • Analyses du marché.
Aucune restriction	Des informations destinées à une diffusion générale, ou qui ne sont pas susceptibles d'avoir un impact sur l'entreprise si elles étaient diffusées.	<ul style="list-style-type: none"> • Documents de marketing. • Publications. • Annonces publiques. • Offres d'emploi. • Informations sans impact sur Barclays.

Tableau B2 : Schéma d'étiquetage des informations Barclays – exigences de gestion

*** Les informations relatives à la configuration de la sécurité des systèmes, les résultats d'audit, et les dossiers personnels peuvent être classés comme des informations restreintes – internes ou secrètes, en fonction de l'impact qu'une divulgation non autorisée aurait sur l'entreprise.

Étape du cycle de vie	Restreintes - internes	Restreintes - externes	Secrètes
Création et introduction	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs. 	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs. 	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs.
Stockage	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones publiques (y compris les zones publiques au sein des locaux auxquelles les visiteurs peuvent accéder sans supervision). Les informations ne doivent pas être conservées dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision. 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs. 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs. Toutes les clés utilisées pour protéger les données, l'identité et/ou la réputation de Barclays doivent être protégées par des modules de sécurité matérielle certifiés FIPS 140-2 niveau 3 ou plus.

<p>Accès et utilisation</p>	<ul style="list-style-type: none"> • Les actifs (physiques ou électroniques) ne doivent pas être laissés dans des zones publiques en dehors des locaux. • Les actifs (physiques ou électroniques) ne doivent pas être conservés dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique si nécessaire. 	<ul style="list-style-type: none"> • Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). • Les actifs imprimés doivent être récupérés immédiatement de l'imprimante. Si cela n'est pas possible, des outils d'impression sécurisés doivent être utilisés. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique. 	<ul style="list-style-type: none"> • Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). • Les actifs imprimés doivent l'être au moyen d'outils d'impression sécurisés. • Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique.
<p>Partage</p>	<ul style="list-style-type: none"> • Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. • Les actifs électroniques doivent porter une étiquette d'information clairement visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. 	<ul style="list-style-type: none"> • Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible. • Les actifs électroniques doivent porter une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. 	<ul style="list-style-type: none"> • Une étiquette d'information visible doit être apposée sur chaque page des actifs physiques. • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible et être scellées avec un sceau inviolable. Elles doivent être placées à l'intérieur d'une deuxième enveloppe non étiquetée avant distribution. • Les actifs électroniques doivent porter une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation.

	<ul style="list-style-type: none"> Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. 	<ul style="list-style-type: none"> Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. Les actifs doivent être distribués uniquement aux individus qui ont besoin de les recevoir. Les actifs ne doivent pas être télécopiés, à moins que l'expéditeur se soit assuré que les destinataires sont prêts à les récupérer. Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne. 	<ul style="list-style-type: none"> Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. Les actifs doivent être distribués uniquement aux individus spécialement autorisés par le propriétaire des informations à les recevoir. Les actifs ne doivent pas être télécopiés. Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne. Pour les actifs électroniques, une chaîne de responsabilité doit être observée.
Archivage et destruction	<ul style="list-style-type: none"> Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. 	<ul style="list-style-type: none"> Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. 	<ul style="list-style-type: none"> Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. Les supports sur lesquels des actifs électroniques secrets ont été stockés doivent être nettoyés de façon appropriée avant ou pendant la destruction.

Annexe C : Espace bancaire dédié – Exigences de contrôle (NB: vérifiez avec votre représentant chargé de l'approvisionnement, si nécessaire.)

Domaine du contrôle	Intitulé du contrôle	Description du contrôle
Espace bancaire dédié	Séparation physique	La zone physique occupée doit être dédiée à Barclays et ne doit pas être partagée avec d'autres entreprises/fournisseurs.
Espace bancaire dédié	Contrôle de l'accès physique	Des contrôles automatiques sécurisés doivent être en place pour accéder à l'espace bancaire dédié, y compris : 1) Pour le personnel autorisé ; i) Badge avec photo, visible en permanence ii) Pose de lecteurs de carte de proximité iii) Activation d'un mécanisme anti-retour 2) Pour les visiteurs/fournisseurs i) Émargement d'un registre de visite i) Badge à utilisation restreinte, visible en permanence
Espace bancaire dédié	Contrôle de l'accès physique	Les alarmes doivent être configurées de manière à signaler les incidents via un système d'accès centralisé avec contrôle d'accès auditable.
Espace bancaire dédié	Contrôle de l'accès physique et nettoyage	Les contrôles doivent être surveillés, afin de s'assurer qu'un accès adéquat à l'espace bancaire dédié ou aux autres zones critiques est accordé. Seul le personnel autorisé des entreprises de nettoyage et des services techniques (électriciens, techniciens en climatisation, équipes de nettoyage, etc.) doit avoir accès à l'espace bancaire dédié.
Espace bancaire dédié	Accès à distance – Identification et vérification	Tout utilisateur doit uniquement s'authentifier sur le réseau Barclays depuis l'espace bancaire dédié en utilisant un jeton d'authentification multifacteur fourni par Barclays.
Espace bancaire dédié	Accès à distance – Jetons logiciels	L'installation des jetons logiciels ou d'un logiciel RSA doit être effectuée par des membres autorisés du personnel dans l'espace bancaire dédié approuvé, sur les postes de travail.
Espace bancaire dédié	Accès à distance – Assistance en cas d'absence	L'accès à distance à l'environnement de l'espace bancaire dédié n'est pas assuré par défaut pour toute assistance en cas d'absence du bureau ou en dehors des heures de travail. Tout accès à distance doit être approuvé par les équipes Barclays concernées (y compris le Responsable de la sécurité).

Espace bancaire dédié	E-mail et Internet	La connexion au réseau doit être sécurisée et restreindre les activités liées aux e-mails et à Internet sur le réseau de l'espace bancaire dédié.
Espace bancaire dédié	Environnements de développement de logiciels, de test et de développement	Le fournisseur doit s'assurer que le développement de logiciels est réalisé uniquement pour les programmes possédés par Barclays au sein de l'espace bancaire dédié.
Espace bancaire dédié	Contrôles du réseau – Transmission	Toutes les informations doivent être transmises de manière sécurisée entre l'environnement de l'espace bancaire dédié et Barclays, et les périphériques réseau doivent être gérés au moyen de protocoles sécurisés.
Espace bancaire dédié	Contrôles du réseau – Routage	Le routage doit être configuré de telle sorte que les connexions sont établies uniquement avec le réseau de Barclays, et qu'elles ne sont pas routées vers d'autres réseaux.
Espace bancaire dédié	Contrôles du réseau – Réseaux sans fil	Les réseaux sans fil ne doivent pas être utilisés dans le segment de réseau de Barclays pour fournir les services.

Secret bancaire

Contrôles supplémentaires
uniquement pour les juridictions
autorisant le secret bancaire
(Suisse/Monaco)

Domaine/intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Rôles et responsabilités	<p>Le fournisseur doit définir et communiquer les rôles et responsabilités relatifs à la gestion des données d'identification des clients (ci-après DIC). Le fournisseur doit examiner les documents décrivant les rôles et responsabilités relatifs aux DIC après chaque changement substantiel apporté au modèle d'exploitation (ou à l'activité) du fournisseur ou au moins une fois par an et les distribuer auprès de la juridiction autorisant le secret bancaire concernée.</p> <p>Les rôles clés doivent comprendre un cadre supérieur, responsable de la protection et la surveillance de l'ensemble des activités relatives aux DIC (Veuillez vous référer à l'Annexe A pour connaître la définition de DIC)</p>	<p>La définition claire des rôles et des responsabilités soutient la mise en œuvre de l'annexe Obligations de contrôle pour les fournisseurs externes.</p>
2. Signalement de violation de DIC	<p>Des contrôles et processus documentés doivent être en place pour assurer le signalement et la gestion de toute violation ayant un impact sur des DIC.</p> <p>Toute violation des exigences de gestion (ainsi qu'il est défini au tableau B2) doit faire l'objet d'une réponse du fournisseur et être signalée immédiatement à la juridiction autorisant le secret bancaire correspondante (au plus tard sous 24 heures). Un processus de réponse en cas d'incident destiné à gérer en temps opportun et à signaler régulièrement les événements impliquant des DIC doit être défini.</p> <p>Le fournisseur doit s'assurer que les mesures correctives identifiées à la suite d'un incident sont traitées selon un plan correctif (action, propriété, date de livraison), et partagées et approuvées par la juridiction autorisant le secret bancaire correspondante.</p>	<p>L'existence d'un processus de réponse en cas d'incident aide à assurer la maîtrise rapide et à éviter l'aggravation des incidents.</p> <p>Toute violation ayant un impact sur des DIC peut porter gravement atteinte à la réputation de Barclays et entraîner des amendes et une perte de l'agrément bancaire en Suisse ou à Monaco.</p>

<p>3. Formation et sensibilisation</p>	<p>Les employés du fournisseur qui ont accès à des DIC et/ou les gèrent doivent suivre une formation* qui met en œuvre les exigences relatives au secret bancaire des DIC après toute nouvelle modification des réglementations ou au moins une fois par an.</p> <p>Le fournisseur doit s'assurer que tous ses nouveaux employés (qui ont accès à des DIC et/ou les gèrent), suivent, dans un délai raisonnable (environ 3 mois), une formation pour s'assurer qu'ils comprennent leurs responsabilités eu égard aux DIC.</p> <p>Le fournisseur doit assurer un suivi des employés qui ont suivi la formation.</p> <p>* les juridictions autorisant le secret bancaire fourniront des orientations sur le contenu attendu de la formation.</p>	<p>La formation et la sensibilisation viennent à l'appui de tous les autres contrôles présentés dans cette annexe.</p>
<p>4. Schéma d'étiquetage des informations</p>	<p>Le cas échéant*, le fournisseur doit appliquer le schéma d'étiquetage des informations Barclays (Tableau D1 de l'Annexe D), ou un autre programme convenu avec la juridiction autorisant le secret bancaire, à l'ensemble des actifs informationnels détenus ou traités pour le compte de la juridiction autorisant le secret bancaire.</p> <p>Les exigences de gestion des données DIC sont stipulées au Tableau D2 de l'Annexe D.</p> <p>* « le cas échéant » fait référence à l'avantage qu'apporte l'étiquetage par rapport au coût associé. Par exemple, l'étiquetage d'un document n'est pas approprié si cela conduit à la violation des exigences anti-violation réglementaires.</p>	<p>L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés.</p>
<p>5. Cloud Computing/storage externe</p>	<p>Toute utilisation du cloud computing et/ou d'un stockage externe des DIC (sur des serveurs en dehors de la juridiction autorisant le secret bancaire ou en dehors de l'infrastructure du fournisseur) dans le cadre du service offert à ladite juridiction doit être approuvée par les équipes locales concernées correspondantes (y compris le Responsable de la sécurité, les services Conformité et Juridique) ; et des contrôles doivent être mis en œuvre conformément à la juridiction autorisant le secret bancaire correspondante pour protéger dûment les informations DIC eu égard au profil de risque élevé qu'elles présentent.</p>	<p>Le non-respect de ce principe risque de compromettre les données clients (DIC) incorrectement protégées, ce qui peut se traduire par une sanction légale ou réglementaire, ou une atteinte à la réputation.</p>

** Les données d'identification des clients sont des données particulières en raison des lois relatives au secret bancaire en vigueur en Suisse et à Monaco. À ce titre, les contrôles énumérés ici viennent compléter ceux énumérés ci-dessus.

Terme	Définition
DIC	Données d'identification des clients
CSSI	Cybersécurité et sécurité des informations
Employé du fournisseur	Toute personne directement affectée au fournisseur en tant qu'employé permanent, ou toute personne fournissant des services au fournisseur pendant une période limitée (comme un consultant)
Actif	Une information ou un groupe d'informations qui présente une valeur pour l'organisation.
Système	Dans le cadre du présent document, un système se compose de personnes physiques, de procédures, d'équipements informatiques et de logiciels. Les éléments de cette entité complexe sont utilisés en combinaison dans l'environnement opérationnel ou d'assistance visé pour exécuter une tâche donnée ou atteindre un objectif spécifique, fournir une assistance ou satisfaire les exigences d'une mission.
Utilisateur	Un compte attribué à un employé, consultant, sous-traitant ou travailleur intérimaire du fournisseur qui dispose d'un accès autorisé à un système appartenant à Barclays sans privilèges étendus.

Annexe D : DÉFINITION DE DONNÉES D'IDENTIFICATION DES CLIENTS

Les **DIC directes (DICD)** peuvent être définies comme des identifiants uniques (détenus par le client) qui permettent, en tant que tels et d'eux-mêmes, d'identifier un client sans accéder aux données figurant dans les applications bancaires Barclays. Ceci ne doit pas être ambigu, ni sujet à interprétation, et peut comprendre des informations comme le prénom, le nom, le nom de la société, la signature, l'ID au sein du réseau social, etc. Les DIC directes désignent des données clients qui ne sont pas détenues ni créées par la banque.

Les **DIC indirectes (DICI)** sont réparties en 3 niveaux

- Les **DICI N1** peuvent être définies comme des identifiants uniques (détenus par la banque) qui permettent d'identifier individuellement un client si un accès aux applications bancaires ou à d'autres **applications tierces** est fourni. L'identificateur ne doit pas être ambigu, ni sujet à interprétation, et peut comprendre des identifiants comme le numéro de compte, le code IBAN, le numéro de carte de crédit, etc.
- Les **DICI N2** peuvent être définies comme des informations (détenues par le client) qui, associées à d'autres, permettraient de déduire l'identité d'un client. Alors que ces informations ne peuvent pas être utilisées seules pour identifier un client, elles peuvent être utilisées avec d'autres informations pour identifier un client. Les DICI N2 doivent être protégées et gérées avec la même rigueur que les DICD.
- Les **DICI N3** peuvent être définies comme des identifiants uniques mais anonymisés (détenus par la banque) qui permettent d'identifier un client si un accès aux applications bancaires est fourni. La différence avec les DICI N1 est que les informations sont classées « Restreintes - externes » au lieu de secret bancaire, à savoir qu'elles ne sont pas soumises aux mêmes contrôles.

Veillez vous référer au Schéma 1 Arbre décisionnel DIC pour obtenir une vue d'ensemble de la méthode de classification.

Les DIC directes et indirectes N1 ne doivent pas être partagées avec des personnes extérieures à la Banque et doivent respecter à tout moment le principe du besoin de connaître. Les DICI N2 peuvent être partagées selon le principe du besoin de connaître, mais ne doivent pas être partagées conjointement avec toute autre DIC. En partageant

plusieurs DIC, il est possible de créer une « association toxique » qui peut potentiellement révéler l'identité d'un client. Nous définissons une association toxique comme comprenant au minimum deux DIC N2. Les DIC N3 peuvent être partagées car elles ne sont pas classées comme des informations de niveau secret bancaire, à moins qu'un usage récurrent du même identifiant ne puisse se traduire par la collecte de données DIC N2 suffisantes pour révéler l'identité du client.

Classification des informations	Secret bancaire		Restreintes - internes	
Classification	DIC directes (DICD)	DIC indirectes (DICI)		
		Indirectes (N1)	Potentiellement indirectes (N2)	Identifiant impersonnel (N3)
Type d'informations	Nom du client	Numéro du conteneur / ID du conteneur	Prénom	ID de traitement interne
	Nom de la société	Numéro MACC (compte monétaire avec ID conteneur Avaloq)	Date de naissance	Identifiant unique statique
	Relevé de compte	Adresse	Nationalité	Identifiant dynamique
	Signature	Code IBAN	Fonctions	ID conteneur externe
	ID réseau social	Coordonnées de connexion banque électronique	Situation de famille	
	Numéro de passeport	Numéro de coffre	Code postal	
	Numéro de téléphone	Coordonnées de carte de crédit	Situation patrimoniale	

	Adresse e-mail		Nom de famille	
	Intitulé du poste ou intitulé PEP		Dernière visite du client	
	Pseudonyme		Langue	
	Adresse IP		Sexe	
	Numéro de télécopie		Date d'expiration CC	
			Contact principal	
			Lieu de naissance	
			Date d'ouverture du compte	
			Solde/montant d'opération important	

Exemple : Si vous envoyez un courriel ou partagez tout document avec des personnes externes (y compris des tiers en Suisse/à Monaco) ou des collaborateurs internes au sein d'une autre société affiliée/filiale située en Suisse/à Monaco ou dans d'autres pays (par ex. Royaume-Uni)

1. Nom du client
(DICD) = violation du secret bancaire
2. ID conteneur
(DICI N1) = violation du secret bancaire
3. Situation patrimoniale + nationalité
(DICI N2) + (DICI N2) = violation du secret bancaire

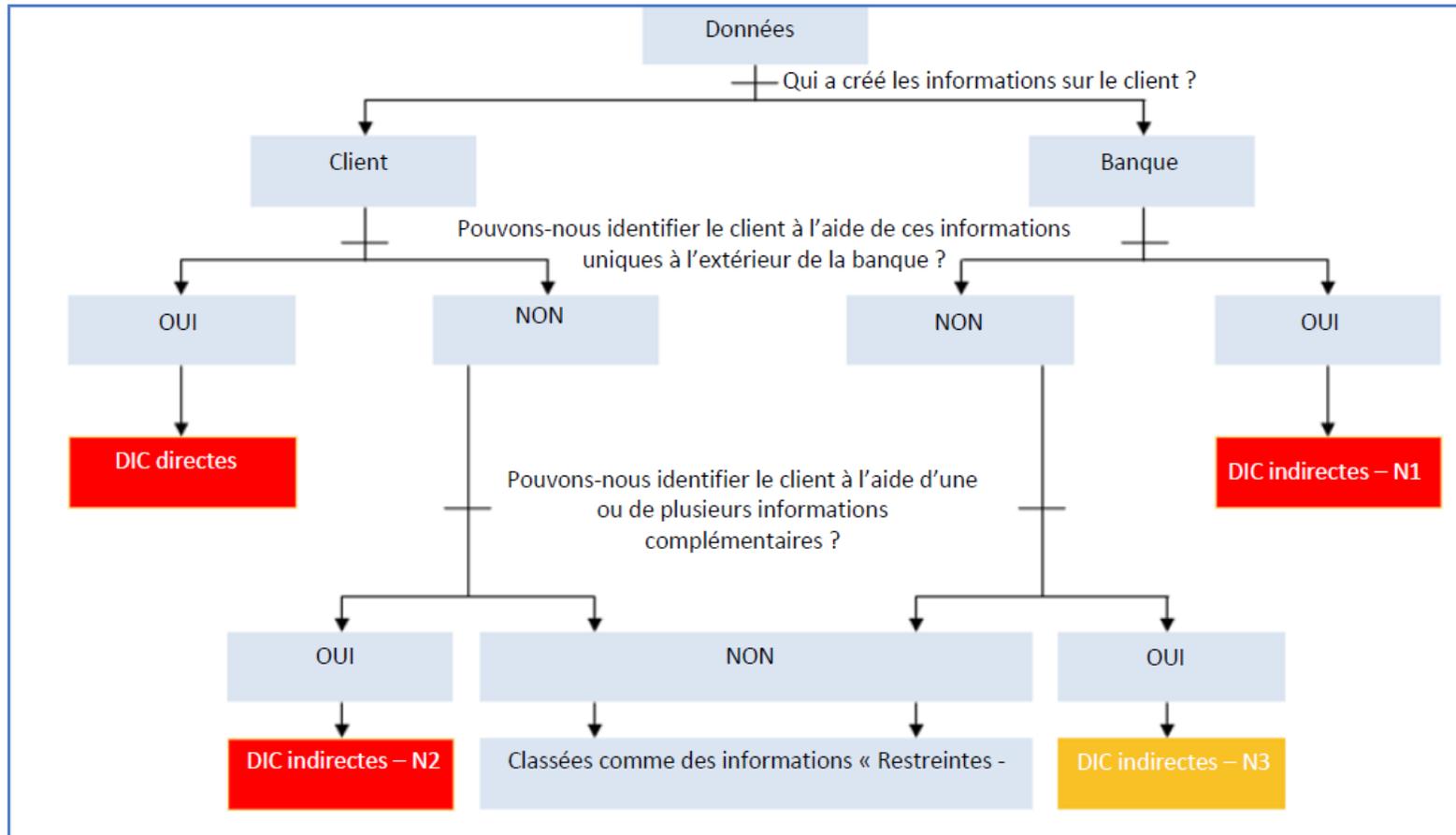


Tableau E1 : Schéma d'étiquetage des informations Barclays

** L'étiquette secret bancaire est propre aux juridictions autorisant le secret bancaire.

Étiquette	Définition	Exemples
Secret bancaire	Informations apparentées à toute donnée d'identification des clients (DIC) directe ou indirecte, suisse. La classification « secret bancaire » s'applique aux Informations apparentées à toute donnée d'identification des clients directe ou indirecte. Par conséquent, un accès par tous les employés, même ceux situés au sein de la juridiction propriétaire, n'est pas approprié. L'accès à ces informations est requis uniquement par les individus qui ont besoin de les connaître pour remplir leurs tâches officielles ou leurs responsabilités contractuelles. Une divulgation, un accès ou un partage non autorisé(e), aussi bien au niveau interne qu'externe de l'entité, desdites informations peut avoir un impact critique et peut entraîner des poursuites pénales et avoir des conséquences civiles et administratives comme des amendes et une perte de l'agrément bancaire, si elles sont divulguées à des membres du personnel non autorisés aussi bien au niveau interne qu'externe.	<ul style="list-style-type: none"> • Nom du client • Adresse du client • Signature • Adresse IP du client (de plus amples exemples figurent à l'Annexe D)

Étiquette	Définition	Exemples
Secrètes	Les informations doivent être classées « secrètes » si leur divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de la structure de gestion des risques d'entreprise (ERMF) comme étant « critique » (financier ou non-financier).	<ul style="list-style-type: none"> • Informations sur les fusions ou acquisitions potentielles. • Informations sur la planification stratégique – commerciale et organisationnelle. • Certaines informations relatives à la configuration de la sécurité des informations.

	<p>Ces informations sont réservées à un public spécifique et ne doivent pas être diffusées ultérieurement sans l'autorisation de l'auteur. Le public peut comprendre des destinataires externes avec l'autorisation explicite du propriétaire des informations.</p>	<ul style="list-style-type: none"> • Certains rapports et résultats d'audit. • Comptes rendus du comité exécutif. • Coordonnées d'authentification ou d'identification et de vérification (ID&V) – client et collaborateur. • Grandes quantités d'informations sur les titulaires de cartes. • Prévisions de bénéfices ou résultats financiers annuels (avant publication officielle). • Tout élément couvert en vertu d'un accord de non-divulgaration (AND) formel.
Restreintes - internes	<p>Les informations doivent être classées « restreintes - internes » si les destinataires prévus sont uniquement des employés authentifiés Barclays et des prestataires de services gérés (PSG) Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique.</p> <p>Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non-financier).</p> <p>Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.</p>	<ul style="list-style-type: none"> • Stratégies et budgets. • Évaluations des performances. • Rémunération du personnel et données personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.
Restreintes - externes	<p>Les informations doivent être classées « restreintes - externes » si les destinataires prévus sont des employés authentifiés Barclays et des PSG Barclays avec un contrat actif en place et ces informations sont réservées à un public spécifique ou à des parties externes qui sont autorisées par le propriétaire des informations.</p> <p>Une divulgation non autorisée est susceptible d'avoir un impact préjudiciable sur Barclays, évalué dans le cadre de l'ERMF comme étant « majeur » ou « limité » (financier ou non-financier).</p>	<ul style="list-style-type: none"> • Plans de nouveaux produits. • Contrats de clients. • Contrats juridiques. • Informations clients individuelles/de petit volume destinées à être envoyées au niveau externe. • Communications avec les clients. • Documentation d'offre de nouvelle émission (par ex. prospectus, notice d'offre). • Documents de recherche finaux. • Informations importantes n'ayant pas été rendues publiques (IIPP) n'appartenant pas à Barclays. • Tous les rapports de recherche • Certains documents de marketing. • Analyses du marché.

	Ces informations ne sont pas destinées à une diffusion générale mais peuvent être transmises ou partagées par des destinataires selon le principe du besoin de connaître.	
Aucune restriction	Des informations destinées à une diffusion générale, ou qui ne sont pas susceptibles d'avoir un impact sur l'entreprise si elles étaient diffusées.	<ul style="list-style-type: none"> • Documents de marketing. • Publications. • Annonces publiques. • Offres d'emploi. • Informations sans impact sur Barclays.

Tableau E2 : Schéma d'étiquetage des informations – exigences de gestion

** Les exigences de gestion spécifiques des données DIC pour garantir leur confidentialité conformément aux exigences réglementaires

Étape du cycle de vie	Exigences relatives au secret bancaire
Création et étiquetage	<p>Comme pour « Restreintes - externes » et :</p> <ul style="list-style-type: none"> • Un propriétaire des DIC doit être affecté aux actifs.
Stockage	<p>Comme pour « Restreintes - externes » et :</p> <ul style="list-style-type: none"> • Les actifs doivent être stockés sur des supports amovibles uniquement pendant la durée explicitement requise par un besoin commercial spécifique, les organismes de réglementation ou des auditeurs externes. • Les volumes importants d'actifs informationnels relevant du secret bancaire ne doivent pas être stockés sur des appareils/supports portables. Pour obtenir de plus amples informations, veuillez contacter l'équipe cybersécurité et sécurité des informations locale (ci-après CSSI). • Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder, selon le principe du besoin de connaître ou du besoin d'avoir. • Des pratiques de sécurisation du lieu de travail comme un bureau bien rangé et un verrouillage de l'ordinateur de bureau doivent être observées pour protéger les actifs (physiques ou électroniques). • Les actifs informationnels sur des supports amovibles doivent être utilisés pour stockage uniquement pendant la durée explicitement requise, et doivent être conservés sous clé lorsqu'ils ne sont pas utilisés. • Les transferts de données ponctuels vers des appareils/supports portables exigent l'autorisation du propriétaire des données, du service conformité et de l'équipe CSSI.
Accès et utilisation	<p>Comme pour « Restreintes - externes » et :</p> <ul style="list-style-type: none"> • Les actifs ne doivent pas être emportés / visualisés en dehors du site (locaux Barclays) sans l'autorisation formelle du propriétaire des DIC (ou son adjoint). • Les actifs ne doivent pas être emportés / visualisés en dehors de la juridiction de tenue des registres du client sans l'autorisation formelle du propriétaire des DIC (ou son adjoint) et du client (décharge/pouvoir limité). • Des pratiques de sécurisation du télétravail, en s'assurant qu'aucun espionnage par-dessus l'épaule n'est possible, doivent être observées lorsque des actifs physiques sont emportés en dehors du site.

	<ul style="list-style-type: none"> S'assurer que les personnes non autorisées ne peuvent pas observer ou accéder aux actifs électroniques contenant des DIC en utilisant un accès restreint aux applications d'entreprise.
Partage	<p>Comme pour « Restreintes - externes » et :</p> <ul style="list-style-type: none"> Les actifs doivent être distribués uniquement en se conformant au « principe du besoin de connaître » ET au sein des systèmes d'information et du personnel de la juridiction d'origine autorisant le secret bancaire. Les actifs transférés ponctuellement au moyen de supports amovibles exigent l'autorisation du propriétaire des actifs informationnels et de l'équipe CSSI. Les communications électroniques doivent être chiffrées pendant leur transit. Les actifs (copie papier) envoyés par courrier doivent être expédiés au moyen d'un service exigeant un accusé de réception. Les actifs doivent être distribués uniquement en se conformant au « principe du besoin de connaître ».
Archivage et destruction	Comme pour « Restreintes - externes »

*** Les informations relatives à la configuration de la sécurité des systèmes, les résultats d'audit, et les dossiers personnels peuvent être classés comme des informations restreintes – internes ou secrètes, en fonction de l'impact qu'une divulgation non autorisée aurait sur l'entreprise.

Étape du cycle de vie	Restreintes - internes	Restreintes - externes	Secrètes
Création et introduction	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs. 	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs. 	<ul style="list-style-type: none"> Un propriétaire des informations doit être affecté aux actifs.
Stockage	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones publiques (y compris les zones publiques au sein des locaux auxquelles les visiteurs peuvent accéder sans supervision). 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être stockés dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder.

	<ul style="list-style-type: none"> Les informations ne doivent pas être conservées dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision. 	<ul style="list-style-type: none"> Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs. 	<ul style="list-style-type: none"> Les actifs électroniques stockés doivent être protégés par chiffrement ou par des contrôles compensatoires appropriés s'il existe un risque significatif que des individus non autorisés puissent accéder à de tels actifs. Toutes les clés utilisées pour protéger les données, l'identité et/ou la réputation de Barclays doivent être protégées par des modules de sécurité matérielle certifiés FIPS 140-2 niveau 3 ou plus.
Accès et utilisation	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être laissés dans des zones publiques en dehors des locaux. Les actifs (physiques ou électroniques) ne doivent pas être conservés dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision. Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique si nécessaire. 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). Les actifs imprimés doivent être récupérés immédiatement de l'imprimante. Si cela n'est pas possible, des outils d'impression sécurisés doivent être utilisés. Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique. 	<ul style="list-style-type: none"> Les actifs (physiques ou électroniques) ne doivent pas être manipulés ou laissés sans surveillance dans des zones où des individus non autorisés ont la possibilité de les consulter ou d'y accéder. Les actifs peuvent être manipulés si des contrôles adaptés sont en place (par exemple, écrans de confidentialité). Les actifs imprimés doivent être au moyen d'outils d'impression sécurisés. Les actifs électroniques doivent être protégés au moyen de contrôles de gestion de l'accès logique.
Partage	<ul style="list-style-type: none"> Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. 	<ul style="list-style-type: none"> Une étiquette d'information visible doit être apposée sur les actifs physiques. L'étiquette doit figurer au minimum sur la page de titre. 	<ul style="list-style-type: none"> Une étiquette d'information visible doit être apposée sur chaque page des actifs physiques.

	<ul style="list-style-type: none"> • Les actifs électroniques doivent porter une étiquette d'information clairement visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. 	<ul style="list-style-type: none"> • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible. • Les actifs électroniques doivent porter une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. • Les actifs doivent être distribués uniquement aux individus qui ont besoin de les recevoir. • Les actifs ne doivent pas être télécopiés, à moins que l'expéditeur se soit assuré que les destinataires sont prêts à les récupérer. • Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne. 	<ul style="list-style-type: none"> • Les enveloppes contenant des actifs physiques doivent porter à l'avant une étiquette d'information visible et être scellées avec un sceau inviolable. Elles doivent être placées à l'intérieur d'une deuxième enveloppe non étiquetée avant distribution. • Les actifs électroniques doivent porter une étiquette d'information clairement visible. Les copies électroniques de documents de plusieurs pages doivent porter sur chaque page une étiquette d'information visible. • Les actifs doivent être distribués uniquement par le biais de systèmes, de méthodes ou de fournisseurs approuvés par l'organisation. • Les actifs doivent être distribués uniquement aux individus employés par l'organisation, ou sous obligation contractuelle appropriée vis-à-vis de celle-ci, ou dans le cadre d'un besoin commercial clairement reconnu, par exemple dans le cas de la négociation d'un contrat. • Les actifs doivent être distribués uniquement aux individus spécialement autorisés par le propriétaire des informations à les recevoir. • Les actifs ne doivent pas être télécopiés. • Les actifs électroniques doivent être chiffrés au moyen d'un mécanisme de protection cryptographique approuvé lorsqu'ils transitent en dehors du réseau interne. • Pour les actifs électroniques, une chaîne de responsabilité doit être observée.
--	--	---	--

Archivage et destruction	<ul style="list-style-type: none"> • Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. 	<ul style="list-style-type: none"> • Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. 	<ul style="list-style-type: none"> • Les actifs physiques doivent être détruits en utilisant un service de mise au rebut confidentiel. • Les copies des actifs électroniques doivent également être supprimées de la « corbeille » du système ou autres emplacements similaires en temps opportun. • Les supports sur lesquels des actifs électroniques secrets ont été stockés doivent être nettoyés de façon appropriée avant ou pendant la destruction.
---------------------------------	--	--	---