Obligations de contrôle pour les fournisseurs externes

Sécurité des informations et cybersécurité

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

Version 9.0 - Avril 2019

Intitulé du contrôle	Description du contrôle	Raisons de l'importance
1. Gouvernance, politique et normes en matière de sécurité des informations/cybersécurité	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 et de cybersécurité, ainsi qu'un programme de sécurité destiné à protéger le fournisseur contre toute 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. Le fournisseur doit évaluer régulièrement les risques liés à la sécurité des informations/cybersécurité et mettre en œuvre les contrôles et les étapes requis pour réduire les risques identifiés. 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. Le fournisseur doit définir les rôles et responsabilités relatifs à la sécurité des informations/ cybersécurité.	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. 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.
2. Processus de gestion des incidents	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 : • 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. • 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 communiquées à Barclays.	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.

3. Sécurité des points d'extrémité	Le fournisseur doit s'assurer que les points d'extrémité utilisés pour accéder au réseau de Barclays ou pour traiter des données de Barclays doivent être renforcés à des fins de protection contre les attaques. 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.	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.
4. 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 auprès de Barclays doit être dûment protégée. 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.
5. Protection contre les logiciels malveillants	Des contrôles et des outils contre les logiciels malveillants doivent être en place afin d'offrir une protection adéquate contre les logiciels malveillants tels que les virus et autres.	Les solutions contre les logiciels malveillants sont cruciales pour la protection des actifs informationnels Barclays contre les codes malveillants.
6. Sécurité du réseau	Le fournisseur doit s'assurer que l'ensemble des systèmes informatiques exploités par le fournisseur ou son sous-traitant qui soutiennent les services fournis à Barclays sont protégés contre un mouvement latéral de menaces au sein du réseau du fournisseur (et de tout sous-traitant concerné). Les mécanismes de protection suivants doivent être pris en compte par le fournisseur selon le(s) service(s) qu'il fournit à Barclays : **Connexions externes :** Toutes les connexions externes au réseau doivent être documentées, routées via un pare-feu, et vérifiées et approuvées avant d'être établies, afin de prévenir les violations de la sécurité des données. **Accès sans fil :** Tout accès sans fil au réseau doit être protégé par des protocoles de chiffrement, de séparation, d'authentification et d'autorisation pour prévenir les violations de la sécurité.	Le non-respect de ce principe peut se traduire par l'exploitation des réseaux internes ou externes par des pirates afin d'accéder au service ou aux données.

	Prévention/détection des intrusions : Des outils et des systèmes de prévention et de détection des intrusions doivent être déployés en tout point approprié du réseau, et les résultats doivent être surveillés en conséquence afin de détecter toute atteinte à la cybersécurité, y compris les menaces persistantes avancées (APT). **Déni de service distribué (DDoS) :** Une approche approfondie de la défense doit être mise en œuvre sur le réseau et les systèmes clés pour offrir une protection constante contre les interruptions de service dues à des cyberattaques. *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.*	
7. Protection des applications	Le développement des logiciels / applications du fournisseur doit s'assurer que toutes les activités de sécurité clés ont été intégrées au processus de développement des logiciels, afin de prévenir les interruptions de service, les vulnérabilités de sécurité et les violations de la cybersécurité. 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. Le fournisseur doit s'assurer que le code source est exécuté, stocké et envoyé à Barclays de manière sécurisée.	Les contrôles protégeant le développement d'applications aident à s'assurer que les applications sont sécurisées au moment du déploiement.
8. Simulation de menaces / tests de pénétration / évaluation de la sécurité informatique	Le fournisseur doit faire appel à un prestataire de services de sécurité qualifié indépendant pour réaliser une évaluation de la sécurité informatique/des tests de pénétration portant sur l'infrastructure et les applications informatiques se rapportant au(x) service(s) que le fournisseur fournit à Barclays. 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.	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.

	Le fournisseur doit utiliser un mécanisme cohérent pour enregistrer, trier, et répondre aux vulnérabilités identifiées.	
9. Technologies de protection des actifs et de la sécurité	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. 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). Les actifs ou les systèmes stockant ou traitant ces derniers doivent être protégés contre tout(e) altération physique, perte, dommage ou saisie et toute configuration ou modification inappropriée. Les actifs informationnels de 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. Les systèmes doivent être configurés de manière sécurisée pour prévenir toute violation inutile. La surveillance, l'audit et la consignation des systèmes doivent être en place afin de détecter toute activité inappropriée ou malveillante.	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.

10. Gestion de l'accès logique (LAM)	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. • 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 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.	L'existence de contrôles de la gestion de l'accès logique appropriés aide à assurer la protection des actifs informationnels contre toute utilisation inappropriée.

	Ces principes doivent être appliqués en fonction des risques, en prenant en compte le niveau de confidentialité des informations. Chaque compte doit être associé à une seule personne, qui sera responsable de toute activité conduite en utilisant ce compte. Cela n'empêche pas l'utilisation de comptes partagés, mais une seule personne doit quand même être responsable de chaque compte partagé. Les processus de gestion de l'accès seront définis conformément aux bonnes pratiques de l'industrie et incluront, au minimum, les éléments ci-après : • processus d'autorisation robuste en place avant la création/modification/suppression de comptes ; • processus d'examen périodique de l'accès des utilisateurs ; • contrôles des employés mutés – accès modifié/supprimé dans les 5 jours ouvrables suivant la date de la 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 du 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. • 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. 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.).	
11. Prévention des fuites de données	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.	Les contrôles de prévention des fuites de données appropriés constituent un élément crucial de la sécurité des informations, en ce

	Les canaux de fuite de données suivants doivent être pris en compte : • 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) ; • échange d'informations non sécurisé avec des tiers ; et • impression ou copie inappropriée d'informations	qu'ils contribuent à assurer l'absence de pertes d'informations Barclays.
12. Schéma d'étiquetage des informations	***Le cas échéant****, le fournisseur doit appliquer le schéma d'étiquetage des informations Barclays et les exigences de gestion (Annexe B, Tableau B1 et B2), ou un autre programme convenu avec Barclays, à l'ensemble des actifs informationnels détenus ou traités pour le compte de Barclays. * « ***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.*	L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés.
13. Droit d'inspection	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. 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.	Si cela n'est pas convenu, les fournisseurs seront dans l'incapacité de présenter toutes les garanties de respect de ces obligations de sécurité.

Annexe A : Glossaire

Définition	
Actif informationnel	Toute information caractérisée par une certaine valeur en termes de confidentialité, d'intégrité et de disponibilité. Une information ou un groupe d'informations qui présente une valeur pour l'organisation. Généralement regroupé à un niveau (processus d'entreprise) élevé.
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).
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
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.
Menaces persistantes avancées (MPA)	Une menace persistante avancée (MPA) est une attaque furtive de réseau informatique où une personne ou un groupe obtient un accès non autorisé à un réseau sans être détecté(e) pendant une période prolongée.
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.
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	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). 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.	• 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 • 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	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. 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). 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.	• Stratégies et budgets. • Évaluations des performances. • Rémunération du personnel et données personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.
Restreintes - externes	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	• Plans de nouveaux produits. • Contrats de clients. • Contrats juridiques.

	à un public spécifique ou à des parties externes qui sont autorisées par le propriétaire des informations. 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). 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.	• 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.	• 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	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.
Stockage	• 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 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 (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.

	• Les informations ne doivent pas être conservées dans des zones publiques dans les locaux auxquelles les visiteurs peuvent accéder sans supervision.	• 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	• 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.	• 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.	• 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.
Partage	• 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. • 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.	• 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.	• 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.

		• 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.	• 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	• 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 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 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.

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	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. 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)	La définition claire des rôles et des responsabilités soutient la mise en œuvre de l'annexe Obligations de contrôle pour les fournisseurs externes.
2. Signalement de violation de DIC	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. Toute violation des exigences de gestion (ainsi qu'il est défini au tableau C2) 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. 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.	L'existence d'un processus de réponse en cas d'incident aide à assurer la maîtrise rapide et à éviter l'aggravation des incidents. 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.

3. Formation et sensibilisation	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. 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. Le fournisseur doit assurer un suivi des employés qui ont suivi la formation. * les juridictions autorisant le secret bancaire fourniront des orientations sur le contenu attendu de la formation.	La formation et la sensibilisation viennent à l'appui de tous les autres contrôles présentés dans cette annexe.
4. Schéma d'étiquetage des informations	***Le cas échéant****, le fournisseur doit appliquer le schéma d'étiquetage des informations Barclays (Tableau C1 de l'Annexe C), 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. Les exigences de gestion des données DIC sont stipulées au Tableau C2 de l'Annexe C. * « ***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.*	L'existence d'un inventaire des actifs informationnels complet et précis est fondamentale pour assurer la mise en œuvre des contrôles appropriés.
5. Cloud Computing/stockage externe	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.	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.

** 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 B : 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.

Veuillez 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 DICI N2. Les DICI 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 DICI 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

Annexe C : Schéma d'étiquetage des informations Barclays

Tableau C1 : 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.	• Nom du client • Adresse du client • Signature • Adresse IP du client (de plus amples exemples figurent à l'Annexe B)

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). 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.	• 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. • 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	Les informations doivent être classées « restreintes - internes » si les destinataires prévus sont uniquement des employés	• Stratégies et budgets.

	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. 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). 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.	• Évaluations des performances. • Rémunération du personnel et données personnelles. • Évaluations de la vulnérabilité. • Rapports et résultats d'audit.
Restreintes - externes	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. 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). 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.	• 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.	• Documents de marketing. • Publications. • Annonces publiques. • Offres d'emploi. • Informations sans impact sur Barclays.

Tableau C2 : 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	Comme pour « Restreintes - externes » et : • Un propriétaire des DIC doit être affecté aux actifs.
Stockage	Comme pour « Restreintes - externes » et : • 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	Comme pour « Restreintes - externes » et : • 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.

	• 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	Comme pour « Restreintes - externes » et : • 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	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.	• Un propriétaire des informations doit être affecté aux actifs.
Stockage	• 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.	• 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.	• 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.
Accès et utilisation	• 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.	• 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.	• 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.

Partage	• 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. • 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.	• 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. • 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.	• 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. • 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	• 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 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 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.