التزامات الرقابة على المورد الخارجي

المعلومات والأمن الإلكتروني

للموردين المصنفين ضمن فئة مخاطر أمن المعلومات والأمن الإلكتروني المرتفعة

إصدار 9.0، بتاريخ مارس 2019

مجال / نطاق الرقابه	وصف الرقابه	الاهميه
1. حوكمة وسياسة ومعايير أمن المعلومات/الأمن الإلكتروني	يتعين على المورد تطبيق عمليات حوكمة المخاطر المعلوماتية/الإلكترونية التي تضمن فهم بيئة التكنولوجيا الخاصة به وحالة ضوابط أمن المعلومات/الأمن الإلكتروني، مع وجود برنامج أمني لحماية المورد من التهديدات المعلوماتية/الإلكترونية وفقًا للممارسات الجيدة الخاصة بمجال تكنولوجيا المعلومات (تشمل NIST وSANS وISO27001) والمتطلبات المطبقة في هذا المجال. يتعين على المورد إجراء عمليات دورية لتقييم المخاطر فيما يتعلق بأمن المعلومات/الأمن الإلكتروني (بما لا يقل عن مرة واحدة كل 12 شهرًا تحت أي ظروف) كما سيطبق ضوابط ويتخذ إجراءات حسب ما يتطلبه الأمر لاحتواء المخاطر التي تم تحديدها.في حال تحديد خطر مادي يمكن أن يؤثر عكسيًا على سمعة بنك باركليز أو الخدمة التي يقدمها، يتعين على المورد إبلاغ البنك. يتعين على المورد الاحتفاظ بسياسات يتم الموافقة عليها من قبل الإدارة العليا، ومعايير لإدارة مخاطر أمن المعلومات والأمن الإلكتروني للمورد، كما يجب مراجعتها مرة واحدة على الأقل في كل سنة.	في حال عدم تنفيذ هذا الضابط، لن يتمكن بنك باركليز أو المورد الخاص به من إظهار قدرتهم على تطبيق الإشراف المناسب على أمن المعلومات والأمن الإلكتروني. السياسات والمعايير الموثقة هي عناصر ضرورية لإدارة المخاطر والحوكمة.فهي تحدد رؤية الإدارة فيما يخص الضوابط المطلوبة لإدارة المخاطر المتعلقة بالمعلومات والأمن الإلكتروني.
2. الاستخدام المتفق عليه	يتعين على المورد وضع ونشر متطلبات الاستخدام المقبول والتي توضح للموظفين العاملين لدى المورد المسؤوليات التي سيتولونها. يجب وضع الموضوعات التالية في الاعتبار: (أ) استخدام الإنترنت؛ (ب) استخدام وسائل التواصل الاجتماعي؛ (ج) استخدام البريد الإلكتروني للشركة؛ (د) استخدام الرسائل الفورية؛ (هـ) استخدام معدات تكنولوجيا المعلومات التي يوفرها المورد؛ (و) استخدام معدات تكنولوجيا المعلومات التي لم يوفرها المورد (مثل الأجهزة الشخصية لكل موظف والتي يحضرها إلى العمل)؛ (ز) استخدام أجهزة التخزين المحمولة/القابلة للإزالة؛ (ح) المسؤوليات أثناء التعامل مع أصول معلومات بنك باركليز؛ (ط) مخرجات قنوات تسرب البيانات يتعين على المورد اتخاذ الإجراءات المناسبة لضمان الالتزام بمتطلبات الاستخدام المقبول.	تساعد متطلبات الاستخدام المقبول على تأسيس بيئة الرقابة التي تحمي أصول المعلومات.

3. الأدوار والمسؤوليات	يجب على المورد تحديد الأدوار والمسؤوليات الخاصة بأمن المعلومات والأمن الإلكتروني وتوصيلها إلى الموظفين.يجب مراجعة هذه التحديدات بصفة دورية (بما لا يقل عن مرة واحدة كل 12 شهرًا تحت أي ظروف) وبعد أي تغيير مادي يطرأ على نموذج تشغيل المورد أو أعماله. ينبغي أن تشمل الأدوار الرئيسية أحد كبار المسؤولين التنفيذيين والمسؤول عن أمن المعلومات والأمن الإلكتروني.	تعريف واضح للأدوار والمسؤوليات التي تدعم تطبيق جدول التزامات الرقابة على المورد الخارجي.
4. الالتزام بالمتطلبات التشريعية والقانونية المحلية	يتعين على المورد التأكد من أن المتطلبات التشريعية والقانونية المرتبطة بأمن المعلومات، والتي تنطبق على دائرة الاختصاص القضائي التي يمارس المورد عمله فيها، متوافقة كما يتأكد من توثيق هذا الامتثال بصورة ملائمة. ملاحظة: يمكن تحديد متطلبات إضافية بواسطة الفرق الإقليمية المرتبطة بوضع تشريعات ولوائح التعاملات البنكية المحلية يجب على الموردين الالتزام بها لدعم بنك باركليز في سويسرا وموناكو.	قد يكون للفشل في الالتزام بالمتطلبات التشريعية والقانونية المحلية أصداء خطيرة على كل من المورد وبنك باركليز ويشمل ذلك دفع غرامات، وقد يصل الأمر في الحالات الجسيمة إلى فقدان البنك لترخيص القيام بالتعاملات البنكية.
5. التثقيف والتوعية	يتعين على المورد توفير التثقيف والتوعية لجميع الموظفين ذوي الصلة.يجب أن يكون التثقيف والتوعية ملائمين لأدوارهم ومسؤولياتهم كما يتعين أن يكون ذلك كافيًا للموظفين ليصبح لديهم القدرة على فهم طبيعة وتحديد الهجمات المحتملة والإبلاغ عن المخاوف المتعلقة بها.وكحد أدنى، يجب أن يتناول التدريب كيفية الحفاظ على الأمن أثناء استخدام الإنترنت (في العمل والمنزل وأثناء السفر)، ومخاطر عمليات الانتحال عن طريق الهندسة الاجتماعية والإجراءات المضادة العملية. يتعين على المورد ضمان استكمال جميع الموظفين (المنضمين/المنتقلين) للتدريب، في غضون فترة زمنية مناسبة، مما يضمن معرفتهم بأدوارهم ومسؤولياتهم ذات الصلة بأمن المعلومات. يجب توفير تدريب محسن للتوعية بأمن المعلومات والأمن الإلكتروني يستهدف مديري الأنظمة وذلك بمعدل سنوي على الأقل وذلك بغرض اطلاعهم على التصورات/التهديدات المتعلقة بدورهم، وكيفية التعرف على تهديدات أمن المعلومات والأمن الإلكتروني وكيفية الحماية من مثل هذه التهديدات وكيفية الإبلاغ عن المخاوف بشأنها.	تدعم عملية التثقيف والتوعية جميع الضوابط الأخرى الموجودة في هذا الجدول. في حال عدم تنفيذ هذا الضابط، لن يكون الموظفون ذوو الصلة على دراية بالمخاطر الإلكترونية واتجاهات الهجمات ولن يستطيعوا اكتشاف أو منع هذه الهجمات.

6. عملية التعامل مع الحوادث	يتعين اتباع وإدارة عملية استجابة للحوادث في وقت مناسب وتقديم التقارير الدورية عن الحوادث التي تشمل معلومات بنك باركليز و/أو الخدمات التي يستعين بها البنك.يجب تعريف ما يلي كجزء من إجراء الاستجابة للحوادث: • الحوادث الأمنية وانتهاكات البيانات التي تؤثر على أو تستهدف أصول بنك باركليز و/أو الخدمات التي يتم تقديمها إلى البنك يجب إبلاغ البنك بها بأسرع ما يمكن مع تقديم تحديثات على التقدم الذي يتم إحرازه في الإجراءات التصحيحية. • يتعين اتباع عملية الاستجابة للحوادث فيما يتعلق بالتعامل مع حالات اختراق أنظمة معلومات باركليز أو الخدمات التي يستخدمها والإبلاغ عنها بصفة دورية في الوقت المناسب. • الانتهاكات غير المعروف مدى تأثيرها على نظام بنك باركليز والإجراءات/التحديثات التصحيحية الخاصة بحل مثل هذه الانتهاكات يجب تقديم تقرير بها إلى البنك بغرض الاطلاع على المعلومات. • يتعين على المورد التأكد من اختبار فرق وعمليات الاستجابة للحوادث، مرة واحد على الأقل كل سنة، للتأكد من قدرة المورد على الاستجابة لحوادث الأمن الإلكتروني التي يتم التعرف عليها.يجب أن يشمل الاختبار التحقق من القدرة على إبلاغ بنك باركليز عن طريق إثبات القدرة على الاتصال بالأشخاص ذوي الصلة. • يجب تحديد عملية وتطبيقها لوضع إجراءات وإدارة عملية احتواء الثغرات الأمنية بعد وقوع حادث أمني دون التخلي عن التحريات أو أنشطة الاستجابة. • يتعين على المورد أن يمتلك عمليات وإجراءات للقيام بتحليل للأسباب الجذرية لكل من الحوادث الداخلية (للمورد) والخارجية. • يتعين على المورد ضمان اتباع الإجراءات التصحيحية المطبقة بعد وقوع حادث من خلال وضع خطة إصلاح (الإجراء والملكية وتاريخ التنفيذ) ومشاركتها مع البنك واعتمادها من جانبه.	تساعد إدارة الحادثة وعملية الاستجابة على التأكد من احتواء الحوادث بسرعة ومنع تصاعد خطورتها.
7. التحسين المستمر	يجب على المورد التعلم باستمرار من الأحداث التي تقع وتطبيق ما تعلمه بهدف تحسين عمليات الدفاع ضد المخاطر الأمنية.	في حال عدم تطبيق هذا الضابط، لن يتمكن الموردون من الاستفادة من الدروس المستفادة من الأحداث السابقة لتحسين وتقوية بيئة التحكم الخاصة بهم.
8. ملكية أصول المعلومات	يتعين على المورد أن يكون لديه جهة اتصال مكلفة بالتنسيق مع مالك أصول معلومات بنك باركليز.	يعد تحديد ملكية أصول المعلومات أمرًا ضروريًا لضمان حماية تلك الأصول.

9. مخطط تعريف المعلومات	**عند اللزوم***، يتعين على المورد تطبيق مخطط تعريف معلومات بنك باركليز ومتطلبات التعامل معها (الملحق "ب"، الجدول "ب1"، و"ب2أ2")، أو مخطط بديل يتم الاتفاق عليه مع البنك، وذلك على جميع أصول المعلومات التي يتم الاحتفاظ بها أو معالجتها بالنيابة عن بنك باركليز. * **"عند اللزوم"** يشير إلى فوائد التعريف بالمعلومات مع ضرورة إحداث توازن مع التكلفة المتضمنة. على سبيل المثال، يعد تعريف مستند ما أمرًا غير مناسبًا، حال كان ذلك مخالفًا للمتطلبات التنظيمية لمكافحة التزوير والتلاعب.	تعد قائمة المخزون الكاملة والدقيقة لأصول المعلومات أمرًا ضروريًا للتأكد من استخدام الضوابط المناسبة.
10. إدارة الأصول	يتعين على المورد الاحتفاظ بقائمة مخزون دقيقة لجميع أصول تكنولوجيا المعلومات الملائمة والمستخدمة لتقديم الخدمة لبنك باركليز ويجب مراجعتها مرة واحدة على الأقل في السنة للتحقق من أن قائمة مخزون أصول تكنولوجيا المعلومات محدثة وكاملة ودقيقة.	في حال عدم تطبيق هذا الضابط، يمكن أن تتعرض أصول بنك باركليز أو الأصول التي يستخدمها المورد لتقديم الخدمة إلى البنك للمخاطر، وهو الأمر الذي قد يؤدي إلى خسائر مالية وفقدان للبيانات والإضرار بالسمعة والتعرض للوم الجهات التنظيمية.
11. التأمين أثناء الإرسال	يتعين حماية أصول معلومات بنك باركليز (ما لم يتم اعتبارها "غير مقيدة" أو ما يساويها) أثناء إرسالها بما يتناسب مع المخاطر المتعلقة بها.	تحمي الضوابط المطبقة أثناء إرسال معلومات بنك باركليز من اعتراضها أو الإفصاح عنها.
12. التخلص من المعلومات المادية والمنطقية والتخلص منها وإخراجها من الخدمة	أصول معلومات بنك باركليز المخزنة إما بصيغة مادية أو إلكترونية، يجب القيام بالتخلص منها أو حذفها بطريقة آمنة تتناسب مع المخاطر المتعلقة بها مع ضمان عدم القدرة على استعادتها.	يساعد التخلص الآمن من أصول المعلومات في التأكد من أن أصول معلومات بنك باركليز لن يتم استعادتها لأي انتهاك لأمن البيانات أو خسارة أعمال أو نشاط ضار.

13. أمن الشبكات	يتعين على المورد أن يتأكد من أن جميع أنظمة تكنولوجيا المعلومات التي يقوم المورد أو مقاوله من الباطن بتشغيلها والتي تدعم الخدمات المقدمة لبنك باركليز محمية من الحركة الجانبية للتهديدات داخل شبكة المورد (وأي مقاولين من الباطن ذوي صلة). يجب أن يضع المورد آليات الحماية التالية في الاعتبار: • من خلال الفصل المنطقي بين منافذ/واجهات استخدام إدارة الأجهزة وعمليات نقل بيانات المستخدمين • ضوابط المصادقة الملائمة • تمكين جميع الضوابط المتاحة لاحتواء الاستغلال وذلك في نظام التشغيل والتطبيقات والعملاء المثبتين. يتعين على المورد تحديد وتشغيل القدرات لاكتشاف الأجهزة غير المسموح بها، والبرامج التي التأكد من أنها ضارة وعالية المخاطر وغير مصرح باستخدامها والموجودة على شبكة المورد. يجب أن يضع المورد أجهزة استشعار في الشبكة لاكتشاف التهديدات في جميع نقاط الدخول والخروج الموجودة بمحيط الشبكة. ملاحظة: يشير المصطلح "شبكة" حسب استخدامه في هذا الضابط إلى أي شبكة غير مملوكة لبنك باركليز والتي يتحمل المورد مسؤوليتها ويشمل شبكة المقاول من الباطن الذي يعمل مع المورد.	في حال عدم تطبيق هذا الضابط، يمكن أن تتعرض الشبكات الداخلية والخارجية لعوامل التهديد.
14. الدفاع المحيط	يتعين على المورد الاحتفاظ بقائمة مخزون لاتصالات الشبكة الخارجية أو وأماكن الاستضافة التي يتم الوصول إليها من خلال الإنترنت وعمليات نقل البيانات المستخدمة لإرسال بيانات بنك باركليز مرة أخرى إلى البنك أو أي أطراف خارجية (ويشمل ذلك على سبيل المثال وليس الحصر أي مقاولين من الباطن يعملون مع المورد). يجب تطبيق تصميم شبكة منفصلة متعددة الأماكن في المحيط بناء على التعرض للمخاطر واحتياجات الأعمال. يجب أن يقتصر وضع الأجهزة في المحيط على تلك الأجهزة التي تتطلب أو تسهل الوصول إلى/من الشبكات الخارجية.	تساعد الحماية الملائمة للمحيط على التأكد من أن الشبكة وأصول معلومات بنك باركليز قد تم تأمينها بطريقة سليمة.
15. الوصول إلى الشبكة والوصول عن بعد	يتعين على المورد التأكد من مراقبة الوصول إلى الشبكة الداخلية وأنه يتم السماح للأجهزة المسموح بها فقط من خلال الضوابط الملائمة التي تتحكم في الوصول إلى الشبكة. في حال السماح بتخزين الوصول عن بعد إلى أصول معلومات بنك باركليز في البيئة التي يديرها المورد، يجب تفعيل المصادقة والتفويض على النقطة النهائية باستخدام عاملين مع الوضع في الاعتبار هوية المستخدم ونوع الجهاز والوضع الأمني للجهاز (مثل مستوى ملفات التصحيح أو أدوات الحماية من البرامج الضارة والأجهزة المحمولة المحمية أو التي تم فك حمايتها، وغيرها). لا يتم توفير الوصول عن بعد لبيئات بنك باركليز بطريقة افتراضية للاتصال من موقع المورد ودعم العمل في غير ساعات الدوام أو أثناء التواجد خارج المكاتب.يجب الحصول على الموافقة على أي اتصال عن بُعد بواسطة فرق بنك باركليز ذات الصلة (ويشمل ذلك كبير المسؤولين عن الأمن).	تساعد ضوابط الوصول إلى الشبكة في التأكد من أن الأجهزة غير الآمنة ليست متصلة بشبكة المورد وهو الأمر الذي قد يؤدي إلى حدوث ثغرات أمنية جديدة.

16. اكتشاف هجمات قطع الخدمة	يتعين على المورد الاحتفاظ بقدرات تتيح له اكتشاف الهجمات التي تهدف إلى قطع الخدمة. يتعين على المورد التأكد من أن القنوات المتصلة بالإنترنت أو القنوات الخارجية التي تدعم الخدمات المقدمة من قبل بنك باركليز يجب أن تتمتع بحماية كافية ضد هجمات قطع الخدمة لضمان إتاحة المعايير المتفق عليها مع البنك.	في حال عدم تطبيق هذا الضابط، قد لا يتمكن بنك باركليز والمورد الخاص به من منع هجمات قطع الخدمة من تحقيق أهدافها.
17. المراقبة/ تسجيل الدخول	يتعين على المورد التأكد من توفر القدرة على مراقبة البنية التحتية لتكنولوجيا المعلومات على مدار 24 ساعة في اليوم و7 أيام في الأسبوع للحد من احتمال وقوع أحداث تهدد الأمن. يتعين على المورد جمع والربط بين بيانات الأحداث من مصادر وأجهزة استشعار النظام المطبق وتحليلها للتعرف على الهجمات/الحوادث وفهم طبيعتها.في حال اكتشاف أي حوادث مادية و/أو انتهاكات لضوابط الأمن، يتعين على المورد التأكد من اتباع عملية إدارة الحوادث (المذكورة في القسم 6 أعلاه). يجب أن يقوم المورد بإعداد جميع الأنظمة الرئيسية وكذلك التطبيقات الرئيسية كي تسجل الأحداث الرئيسية وتضبط الوقت عن طريق المزامنة بين الأنظمة المختلفة باستخدام "بروتوكول وقت الشبكة" (NTP). يجب أن يقوم المورد بتخزين السجلات مركزيًا وتأمينها بطريقة سليمة والاحتفاظ بها لمدة 12 شهرًا بحد أدنى. يجب أن تشمل الأحداث الرئيسية المسجلة تلك الأحداث التي من المحتمل أن تؤثر على سرية وتكامل وإتاحة الخدمات لبنك باركليز وقد يساعد هذا في التعرف على أو التحري عن الحوادث المادية و/أو انتهاكات حقوق الوصول التي تتعلق بأنظمة المورد.	في حال عدم تطبيق هذا الضابط، لن يتمكن الموردون من اكتشاف أو الاستجابة لانتهاكات الأمن الإلكتروني أو استرجاع والتعلم من الأحداث الإلكترونية التي وقعت على شبكاتهم عن طريق تحليل السجلات ذات الصلة.
18. فصل أصول المعلومات	يتعين على المورد تخزين أصول معلومات بنك باركليز على شبكة منفصلة (منطقيًا و/أو ماديًا) عن العملاء الآخرين.	تساعد الشبكة المنفصلة في التأكد أن أصول معلومات بنك باركليز محمية بدرجة كافية تمنع الإفصاح عنها دون تصريح.
19. الحماية من التعليمات البرمجية الخبيثة/ البرامج الضارة	عند توفير الدعم على مستوى نظام التشغيل، يجب أن تملك أنظمة وخدمات وأجهزة تكنولوجيا المعلومات حل لمكافحة البرامج الضارة يتم استخدامه في جميع الأوقات لمنع انقطاع الخدمة أو الانتهاكات الأمنية. يتعين على المورد القيام بما يلي: • إنشاء والحفاظ على حماية محدثة ضد التعليمات البرمجية الخبيثة/ والبرامج الضارة بما يتماشى مع الممارسات الجيدة في هذا المجال (مثل NIST و ISO27001) • توفير الحماية ضد نقل التعليمات البرمجية الخبيثة إلى أنظمة وعملاء بنك باركليز والأطراف الخارجية الأخرى بما يتماشى مع أساليب المعايير المستخدمة في هذا المجال (مثل NIST و ISO27001).	الحلول المضادة للبرامج الضارة ضرورية لحماية أصول معلومات بنك باركليز ضد التعليمات البرمجية الخبيثة.

20. معايير الإصدارات الآمنة ومطابقة التغييرات الأمنية	يتعين على المورد تحديد وتطبيق معايير الإصدارات لجميع البرامج القابلة للتهيئة الجاهزة للاستخدام بشكل مجمع (مثل أنظمة التشغيل وقواعد البيانات) والبرامج الثابتة للبنية التحتية المستخدمة على نطاق واسع (مثل SAN أو أجهزة الشبكة).يجب إصلاح حالات عدم الالتزام بمعايير الإصدارات.يجب أن تخلق التغييرات الأمنية (مثل تغييرات التهيئة الأمنية وتعديل امتيازات الحساب) دائمًا سجل يتم تخزينه في بيئة مضادة للعبث.يجب إجراء مطابقة بين التغييرات المطبقة والتغييرات التي تم التصريح بها. الأنظمة المضيفة وأجهزة الشبكة التي تشكل جزءًا من أنظمة المورد يجب تهيئتها لتعمل بما يتماشى مع الممارسات الجيدة في هذا المجال (مثل NIST وSANS وISO27001).	تساعد ضوابط الإصدارات القياسية في حماية أصول المعلومات من الوصول غير المصرح به. الالتزام بالإصدارات القياسية والضوابط التي تضمن السماح بالتغييرات تساعد على ضمان حماية أصول معلومات بنك باركليز.
21. تكنولوجيات حماية الأمن	يجب تطبيق تكنولوجيات مناسبة للتعامل مع التهديدات الإلكترونية الحالية والناشئة باستخدام خط أساس متسق من الضوابط التي يتم الاحتفاظ بها لمنع تنفيذ وتفعيل واستغلال وانسحاب الهجمات.	في حال عدم تطبيق هذا الضابط، تصبح أصول معلومات بنك باركليز غير محمية بدرجة كافية ضد الهجمات الإلكترونية.
22. أمن نقطة النهاية	يتعين على المورد التأكد من أن نقاط النهاية المستخدمة للوصول إلى شبكة بنك باركليز أو معالجة بياناته مجهزة للحماية من الهجمات. ويشمل ذلك، على سبيل المثال وليس الحصر، تقييد سقف الهجمات من خلال تعطيل البرامج/الخدمات/المنافذ غير اللازمة، والتأكد من أن جميع الإصدارات المستخدمة ما زالت ضمن فترات الدعم العام، والاستعانة بقدرات الحماية ضد البرامج الضارة واستضافة جدار الحماية وتهيئتهم بطريقة صحيحة، ومن اتباع الضوابط لاحتواء محاولات الاستغلال.	في حال عدم تطبيق هذا الضابط، تصبح شبكة بنك باركليز وشبكة المورد ونقاط النهاية معرضة للهجمات الإلكترونية.
23. اكتشاف الأجهزة والبرامج غير المصرح بها	يتعين على المورد التأكد من امتلاكه القدرة والعمليات اللازمة لاكتشاف الأجهزة والبرامج غير المصرح بها، والتي تم التعرف على أنها برامج ضارة وعالية المخاطر وغير مصرح باستخدامها.	في حال عدم تطبيق هذا الضابط، لن يتمكن الموردون من اكتشاف أو إزالة أو تعطيل الجهاز أو البرنامج الضار وغير المصرح به، وهو الأمر الذي يعرّض أصول بنك باركليز لهجمات إلكترونية.
24. منع تسرب البيانات	يجب تقدير خطر تسرب البيانات المرتبطة بالخدمة (الخدمات) التي يوفرها المورد لمخرج بنك باركليز من خلال الشبكة أو الوسيط المادي والعمل على الحد منه. يجب وضع قنوات تسرب البيانات التالية في الاعتبار: • النقل غير المصرح به للمعلومات خارج الشبكة الداخلية/شبكة المورد. • فقدان أو سرقة أصول معلومات بنك باركليز على الوسائط الإلكترونية المحمولة (وتشمل المعلومات الموجودة على أجهزة الكمبيوتر المحمولة، والأجهزة المحمولة، والوسائط القابلة للإزالة) • النقل غير المصرح به للمعلومات إلى الوسائط القابل للإزالة • التبادل غير الآمن للمعلومات مع الأطراف الخارجية (المقاولين من الباطن) • طباعة أو نسخ المعلومات بطريقة غير صحيحة • الأخطاء وحالات الإغفال في تصنيف الأصل وتعريف المعلومات • تسرب المعلومات غير المصرح به عبر "نظام أسماء المجالات" (DNS)	الضوابط الملائمة لمنع تسرب البيانات هي عنصر حيوي لأمن المعلومات، والتي تساعد على ضمان عدم فقدان معلومات بنك باركليز.

25. التخزين الآمن والعملية	يجب اتباع الضوابط لحماية أصول المعلومات (المتعلقة بالخدمة أو الخدمات التي يقدمها المورد إلى بنك باركليز) عند تخزينها أو معالجتها (ينطبق هذا على المعلومات المخزنة كجزء من الأساليب المنظمة وغير المنظمة).	يتم تخزين أصول المعلومات معًا بصورة معتادة وبالتالي تمثل تركيز للمخاطر ويجب تأمينها.
26. عمليات النسخ الاحتياطي واستعادة البيانات	يجب وضع أحكام للتأكد من أن المعلومات يتم نسخها احتياطيًا بشكل كاف واستعادتها بما يتماشى مع المتطلبات المتفق عليها مع مالك أصل معلومات بنك باركليز والحفاظ على أمن أصل المعلومات طوال مدة العملية. يجب الاتفاق على معدل تكرار وطريقة النسخ الاحتياطي مع مالك أصل المعلومات. يجب أن تحدد أصول المعلومات التي تم نسخها احتياطيًا الضوابط لضمان منح حق الوصول فقط عند الحاجة لذلك.	تقوم عمليات النسخ الاحتياطي بتخزين نسخ من أصول المعلومات وبالتالي يجب أن تخضع لنفس الضوابط.

27. إدارة الوصول المنطقي (LAM)	يجب تقييد الوصول إلى المعلومات، ومع مراعاة الاعتبار المستحق لمبدأ "الحاجة إلى المعرفة" ومبدأ "الأقل امتيازًا" وفصل مبادئ الواجبات.مالك أصل المعلومات مسؤول عن اتخاذ قرار يحدد الأشخاص الذين يحتاجون إلى حق الوصول. • معنى مبدأ "الحاجة إلى المعرفة" هو أنه يجب منح حق الوصول إلى المعلومات للأشخاص الذين يحتاجون للمعرفة فقط من أجل تنفيذ مهامهم المسموح بها.على سبيل المثال، إذا كان أحد الموظفين يتعامل بشكل حصري مع العملاء الموجودين في المملكة المتحدة، فهم لا "يحتاجون لمعرفة" المعلومات المتعلقة بالعملاء المقيمين في الولايات المتحدة. • معنى مبدأ "الأقل امتيازًا" هو أنه يجب منح فقط أدنى مستوى من الامتيازات الضرورية إلى الأشخاص من أجل تنفيذ مهامهم المسموح بها.على سبيل المثال، إذا كان أحد الموظفين يحتاج إلى معرفة عنوان العميل ولكن غير مطلوب منه تغيير هذا العنوان، ففي هذه الحالة، يكون "أقل امتياز" يطلبه هو الوصول للقراءة فقط، والذي يجب منحهم إياه بدلاً من حق الوصول مع إمكانية القراءة والكتابة. • يعني مفهوم فصل الواجبات أنه يكون شخصان على الأقل مسؤولان عن الأجزاء المنفصلة لأي مهمة من أجل منع حدوث الأخطاء والاحتيال.على سبيل المثال، الموظف الذي يطلب إنشاء حساب يجب ألا يكون هو الموظف المسؤول عن الموافقة على الطلب. يجب تطبيق هذه المبادئ على أساس المخاطر، مع الوضع في الاعتبار تصنيف سرية المعلومات. يجب أن يقترن كل حساب بشخص مفرد والذي سيكون مسؤولاً عن أي نشاط يتم تنفيذه باستخدام الحساب. لن يعوق هذا استخدام الحسابات المشتركة، ولكن يظل تحديد مسؤولية كل شخص مفرد عن كل حساب مشترك. يجب تحديد عمليات إدارة الوصول وفقًا للممارسات الجيدة في هذا المجال وتشمل العناصر التالية كحد أدنى: • اتباع عملية تفويض قوية قبل إنشاء/تعديل/حذف الحسابات • عملية المراجعة الدورية لوصول المستخدمين مرة واحدة على الأقل في السنة للتحقق من وصول المستخدمين • ضوابط المنقِّل - يتم تعديل/إزالة حقوق الوصول خلال 5 أيام عمل من تاريخ الانتقال • ضوابط التارك - يتم إزالة جميع حقوق الوصول المنطقية لتوفير الخدمات إلى بنك باركليز خلال 24 ساعة من تاريخ الترك، ويتم إزالة جميع حقوق الوصول الثانوية الأخرى خلال 7 أيام • الحسابات الراكدة التي لم يتم استخدامها لمدة 60 يومًا متتالية أو أكثر يجب تعليق العمل بها.	تساعد الضوابط المناسبة لإدارة الوصول المنطقي على التأكد من أن أصول المعلومات محمية من الاستخدام غير الملائم.

28. أساليب الوصول	يجب تتبع الأنشطة التي تتم باستخدام حساب لضمان أن شخص واحد فقط هو الذي يقوم بذلك.يجب تطبيق العملية والإجراءات الفنية لفرض المستوى المناسب من الوصول إلى أصل المعلومات. يجب أن تتناسب الضوابط الأمنية المتعلقة بالحسابات (مثل المصادقة القوية أو عمليات منح حقوق الوصول في حالة الطوارئ) مع المخاطر التي قد يتعرض لها الحساب أو لإساءة استخدامه. يجب تحديد أسلوب الوصول وفقًا للممارسات الجيدة في هذا المجال وتشمل العناصر التالية كحد أدنى: • ينبغي تغيير كلمات مرور الحسابات التفاعلية كل 90 يومًا على الأقل، كما ينبغي أن تكون كلمة المرور مختلفة عن كلمات المرور الاثنتي عشرة (12) السابقة. • يجب تغيير الحسابات المميزة بعد كل استخدام، وكل 90 يومًا كحد أدنى. • ينبغي تعطيل الحسابات التفاعلية بعد خمس (5) محاولات خاطئة متتالية كحد أقصى. ينبغي السماح بالوصول عن بعد إلى خدمات بنك باركليز عبر آليات معتمدة من قبل فرق البنك ذات الصلة، حيث ينبغي تطبيق ذلك باستخدام المصادقة متعددة العوامل.	تساعد ضوابط إدارة الوصول في التأكد من أن المستخدمين المعتمدين فقط هم الذين يمكنهم الوصول إلى أصول المعلومات.
29. حماية التطبيقات	يجب تطوير التطبيقات باستخدام ممارسات آمنة لكتابة التعليمات البرمجية وفي بيئات آمنة.عند قيام المورد بتطوير تطبيقات ليستخدمها بنك باركليز أو التي يتم استخدامها لدعم الخدمة المقدمة إلى البنك، يجب اتباع عمليات وضوابط لتحديد الثغرات الأمنية وإصلاحها في التعليمات البرمجية أثناء عملية التطوير. يجب حماية الملفات الثنائية للتطبيقات من التغييرات غير المصرح بها، أثناء نشرها واستخدامها، ووجوده في مكتبات المصادر. يجب على المورد التأكد من فصل المهام المتعلقة بتطوير الأنظمة، ويشمل ذلك ضمان أن مطوري الأنظمة ليس لديهم حق الوصول إلى بيئة العمل الفعلية، باستثناء حالات الطوارئ التي يكون هذا الوصول محميًا بضوابط كافية مثل إجراءات منح حقوق الوصول في حالة الطوارئ.يتم تسجيل مثل هذه الأنشطة التي تتم في هذه الظروف وتخضع لمراجعة مستقلة.	تساعد الضوابط التي تحمي عملية تطوير التطبيقات على التأكد من أن التطبيقات آمنة أثناء نشرها واستخدامها.

30. التعامل مع الثغرات الأمنية	يتعين على المورد تشغيل آلية منتظمة لتسجيل وفرز الثغرات الأمنية المكتشفة والاستجابة لها. يجب على المورد بناء القدرات لتحديد وتصنيف الثغرات الأمنية في أنظمة وبرامج تكنولوجيا المعلومات بناء على المخاطر عبر جميع المنصات التي تستخدمها المؤسسة. يتعين على المورد التأكد من أن التعامل مع الثغرات الأمنية يتم تغطيته من خلال ممارسة الأعمال بطريقة معتادة في عملياتها التشغيلية وتشمل إجراءات اكتشاف وتقدير مخاطر الثغرات الأمنية للحد من أو إصلاح هذه الثغرات في جميع الأنظمة، ولمنع حدوث ثغرات جديدة أثناء عمليات التغيير ونشر الأنظمة الجديدة. جميع المشاكل الأمنية والثغرات، والتي يمكن أن يكون لها تأثير مادي على أنظمة بنك باركليز أو على الخدمات التي يوفرها المورد للبنك، والتي قرر المورد المخاطرة بقبولها يجب توصيلها إلى بنك باركليز على وجه السرعة والحصول على موافقة مكتوبة من البنك. يجب تثبيت ملفات تصحيح أمن تكنولوجيا المعلومات والتحديثات الخاصة بإصلاح الثغرات الأمنية بواسطة المورد من خلال عملية معتمدة داخلية (يقوم المورد بها) بأسرع وقت لمنع حدوث أي انتهاكات أمنية.أنظمة الموارد التي يتعذر تحديثها لأي سبب يجب أن يكون لديها إجراءات لحماية النظام المعرض للمخاطر.	في حال عدم تطبيق هذا الضابط، قد يستغل المهاجمون الثغرات الأمنية التي تعاني منها الأنظمة لتنفيذ هجمات إلكترونية ضد بنك باركليز والمورد الخاص به.
31. محاكاة التهديدات/اختبار الاختراق/تقييم أمن تكنولوجيا المعلومات	يجب أن يشارك المورد مع موفر خدمات أمنية مؤهل ومستقل لإجراء تقييم لأمن تكنولوجيا المعلومات/ محاكاة للتهديدات تغطي البنية التحتية لتكنولوجيا المعلومات وتطبيقاتها ذات الصلة بالخدمة أو الخدمات التي يقدمها المورد إلى بنك باركليز. يجب تنفيذ هذا الأمر مرة واحدة على الأقل لتحديد الثغرات الأمنية التي يمكن استغلالها لانتهاك سرية بيانات بنك باركليز من خلال الهجمات الإلكترونية.يجب تحديد أولوية لجميع الثغرات الأمنية ومتابعة حلها.أي مشكلة أو جميع المشاكل التي يتم اعتبارها من ضمن المخاطر المقبولة يجب توضيحها والاتفاق عليها مع بنك باركليز. يجب على المورد أن يبلغ ويوافق على نطاق تقييم الأمن مع بنك باركليز، وعلى وجه الخصوص، تاريخ/وقت البداية والنهاية لمنع تعطل الأنشطة الرئيسية لدى بنك باركليز.	في حال عدم تطبيق هذا الضابط، لن يتمكن الموردون من تقدير التهديدات الأمنية التي يواجهونها ومدى ملائمة وقوة دفاعاتهم.

32. إدارة التغيير وملفات التصحيح	يجب حماية بيانات بنك باركليز والأنظمة التي تخزنها أو تعالجها ضد التغييرات غير الملائمة والتي يمكن أن تعرّض إتاحة أو تكامل البيانات للخطر. سيطور المورد ويطبق إستراتيجية لإدارة ملفات التصحيح والتي تدعمها ضوابط الإدارة وإجراءات إدارة ملفات التصحيح والوثائق التشغيلية. وبمجرد أن تصبح ملفات التصحيح الخاصة بأمن تكنولوجيا المعلومات وتحديثات الثغرات الأمنية متاحة يجب تثبيتها من خلال عملية معتمدة في أسرع وقت لمنع أي انتهاكات أمنية.أنظمة الموارد التي يتعذر تحديثها لأي سبب يجب تثبيت إجراءات أمنية عليها لحماية النظام المعرض للمخاطر.يجب إجراء جميع التغييرات بما يتماشى مع عملية إدارة التغيير المعتمدة لدى المورد. يتم فحص تطبيقات المصادر المفتوحة للبحث عن الثغرات الأمنية الخطيرة. يتعين على المورد التأكد من تطبيق الإصلاحات الطارئة بعد إتاحتها واعتمادها ما لم يؤدي هذا إلى حدوث مخاطر أعلى تهدد الأعمال.أنظمة الموارد التي يتعذر تحديثها لأي سبب يجب تثبيت إجراءات أمنية عليها لحماية النظام المعرض للمخاطر بصورة كاملة.يجب إجراء جميع التغييرات بما يتماشى مع عملية إدارة التغيير لدى المورد.	في حال عدم تطبيق هذا الضابط، قد تتعرض الخدمات لمشاكل أمنية تؤثر على بيانات العملاء وتتسبب في فقد الخدمة أو تمكين أنشطة ضارة أخرى.
33. علم التشفير	يتعين على المورد مراجعة وتقييم تكنولوجيا التشفير والخوارزميات التي تستخدمها لضمان أنها ما زالت ملائمة لهذا الغرض.يجب أن تتناسب قوة التشفير المستخدم مع حجم المخاطر، لأنها يمكن أن تؤثر بالسلب على الأداء أو عمليات التشغيل. يجب أن تلتزم عمليات تطبيق التشفير بالمتطلبات والخوارزميات المحددة.	تضمن حماية التشفير الملائمة والمحدثة بالإضافة إلى الخوارزميات توفير الحماية المستمرة لأصول معلومات بنك باركليز.
34. الحوسبة السحابية	جميع أوجه الاستفادة من خدمة الحوسبة السحابية (العامة/الخاصة/المجتمعية/الهجينة) مثل SaaS/PaaS/IaaS المستخدمة كجزء من تقديم الخدمات المتفق عليها إلى بنك باركليز يجب مراجعتها واعتمادها بواسطة فرق البنك المتخصصة (ويشمل ذلك كبير المسؤولين عن الأمن)؛ ويجب أن تتناسب الضوابط الموضوعة لحماية معلومات البنك والخدمة مع حجم المخاطر ومدى أهمية أصل المعلومات لمنع تسرب البيانات والانتهاكات الإلكترونية.	في حال عدم تطبيق هذا المبدأ، يمكن أن تتعرض أصول معلومات بنك باركليز المحمية بطريقة غير مناسبة للخطر مما قد يؤدي إلى توقيع عقوبات قانونية وتنظيمية أو الإضرار بالسمعة.
35. حق التفتيش	سيسمح المورد لبنك باركليز، بعد إرسال البنك لإشعار مكتوب قبل عشرة أيام عمل على الأقل، بإجراء مراجعة أمنية لأي موقع أو تكنولوجيا مستخدمة بواسطة المورد أو مقاوليه من الباطن لتطوير أو اختبار أو تحسين أو تحديث أو تشغيل أنظمة المورد المستخدمة في الخدمات من أجل مراجعة توافق المورد والتزاماته.يجب أن يسمح المورد أيضًا لبنك باركليز بإجراء تفتيش مباشرةً بعد وقوع حادثة أمنية. أي ضوابط غير متوافقة محددة من قبل بنك باركليز تم اكتشافها أثناء التفتيش يجب تقدير مخاطرها بواسطة البنك حتى يتمكن البنك من وضع الإطار الزمني لإصلاح الأخطاء.يقوم المورد بعد ذلك باستكمال أي إصلاحات مطلوبة خلال الإطار الزمني المحدد.سيقدم المورد المساعدة المعقولة بناء على طلب بنك باركليز فيما يتعلق بأي عملية تفتيش.	في حال عدم تطبيق هذا الضابط، لن يتمكن الموردون من توفير الضمان الكامل لتحقيق الالتزامات الأمنية المشار إليها.

36. مساحة مخصصة للبنك	بالنسبة للخدمات المقدمة التي تتطلب مساحة رسمية مخصصة للبنك، يجب اتباع المتطلبات المادية والفنية لمساحة معينة مخصصة للبنك.(إذا كانت المساحة المخصصة للبنك هي أحد متطلبات الخدمة، ستتكون متطلبات الرقابة المذكورة في الملحق "ج" قابلة للتطبيق).	في حال عدم تطبيق هذا الضابط، لا يمكن تطبيق الضوابط المادية والفنية المناسبة وهو الأمر الذي يؤدي لتأخيرات في الخدمة أو تعطلها أو حدوث انتهاكات للأمن الإلكتروني.

الملحق أ: قاموس المصطلحات

التعريفات	
الحساب	هو عبارة عن مجموعة من بيانات الاعتماد (على سبيل المثال، هوية المستخدم وكلمة المرور) والتي يتم من خلالها التحكم في الوصول إلى نظام تكنولوجيا المعلومات عن طريق اتباع ضوابط الوصول المنطقي.
النسخة الاحتياطية، وعملية النسخ الاحتياطي	يشير مصطلح النسخة الاحتياطية أو عملية النسخ الاحتياطي إلى عمل نسخ من البيانات حتى يمكن استخدام هذه النسخ الإضافية لاستعادة البيانات الأصلية بعد وقوع حدث يؤدي لفقد البيانات.
مساحة مخصصة للبنك	تعني المساحة المخصصة للبنك (BDS) أي مرافق في حوزة أو تحت رقابة عضو في مجموعة المورد أو أي مقاول من الباطن يكرس جهوده بطريقة حصرية لبنك باركليز والتي يتم من خلالها أداء أو تقديم الخدمات.
علم التشفير	تطبيق النظرية الرياضية لتطوير أساليب وخوارزميات يمكن تنفيذها على البيانات لضمان تحقيق الأهداف مثل السرية وتكامل البيانات و/أو المصادقة.
قطع الخدمة (هجمة)	هي محاولة لعدم إتاحة موارد الكمبيوتر للمستخدمين المستهدفين.
التخلص/ الحذف	إجراء الكتابة فوق المعلومات أو مسحها أو التخلص منها بطريقة مادية تمنع استعادتها مرة أخرى.
التشفير	تحويل رسالة (بيانات أو صوتية أو فيديو) إلى صيغة غير مفهومة لا يمكن أن يفهمها قراء غير مصرح لهم بذلك. يكون هذا التحويل من صيغة النص العادي إلى صيغة نص مشفر.
أصول المعلومات	أي معلومات ذات قيمة يتم وضعها في الاعتبار من ناحية متطلبات السرية والتكامل والإتاحة.أو أي جزء منفرد من المعلومات أو تجميع للمعلومات له قيمة للمؤسسة.
مالك أصول المعلومات	هو الفرد الموجود داخل المؤسسة والمسؤول عن تصنيف الأصول وضمان التعامل معها بطريقة صحيحة وملائمة.
الأقل امتيازًا	الحد الأدنى من مستوى الوصول أو الأذونات التي تسمح لمستخدم أو لحساب بأداء دورهم في العمل.
التعليمات البرمجية الخبيثة	برامج تمت كتابتها بغرض التحايل على السياسة الأمنية الموضوعة لحماية نظام تكنولوجيا المعلومات أو جهاز أو تطبيق.تشمل الأمثلة فيروسات الكمبيوتر وأحصنة طروادة والفيروسات المتنقلة.
المصادقة متعددة العوامل	المصادقة باستخدام أسلوبين مختلفين أو أكثر للتحقق من صحة المعلومات المقدمة.أحد الأمثلة على ذلك هو استخدام الرمز المميز للأمن، والذي تعتمد المصادقة الناجحة فيه على شيء يمتلكه الشخص (مثل الرمز المميز للأمن) وشيء يعرفه المستخدم (مثل رقم التعريف الشخصي للرمز المميز).
الحساب المميز	هو الحساب الذي يوفر مستوى مرتفع من التحكم في نظام معين لتكنولوجيا المعلومات.وعادة ما تستخدم هذه الحسابات لصيانة النظام أو إدارة الأمن أو تغيير التهيئة في أحد أنظمة تكنولوجيا المعلومات. فعلى سبيل المثال، حسابات "المسؤول" و"الجذر" وUnix ذات معرّف فريد = 0 وحسابات الدعم وحسابات إدارة الأمن وحسابات إدارة الأنظمة وحسابات المسؤول المحلي

حساب مشترك	حساب يتم منحه لواحد أو أكثر من الموظفين أو الاستشاريين أو المقاولين أو العاملين بالوكالة الذي ن لديهم حق وصول مصرح به، ولكن لا يمكن توفير حسابات فردية لكل شخص بسبب طبيعة النظام الذي يتم الوصول إليه.
نظام	النظام، في سياق هذا المستند، عبارة عن أشخاص وإجراءات ومعدات وبرامج تكنولوجيا المعلومات.يتم استخدام عناصر هذا الكيان المركب معًا في البيئة التشغيلية أو بيئة الدعم المستهدفة لأداء مهمة معينة أو تحقيق غرض معين أو دعم أو متطلبات خاصة بإحدى المهام.
مستخدم	حساب مخصص لأحد موظفي المورد أو الاستشاري أو المقاول أو عامل الوكالة الذي يملك حق الوصول المصرح به لنظام دون تمتعه بأي امتيازات عالية المستوى.

الملحق ب: مخطط تعريف معلومات بنك باركليز

الجدول ب1: مخطط تعريف معلومات بنك باركليز

الملصق	التعريف	الأمثلة
سرية	يجب تصنيف المعلومات على أنها "سرية" إذا كان الكشف عنها غير المصرح به سيؤدي إلى أثر عكسي على بنك باركليز يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "حرج" (من الناحية المالية أو غير المالية). يتم تقييد هذه المعلومات لتصبح متاحة لجمهور معين فقط ولا يجب توزيعها إلى أي شخص آخر دون الحصول إلى إذن من المُنشئ.قد يشمل الجمهور مستلمين خارجيين بناء على تفويض صريح من مالك المعلومات.	• معلومات حول عمليات الدمج أو الاستحواذ المحتملة. • معلومات التخطيط الإستراتيجي - الخاصة بالأعمال والمعلومات التنظيمية. • تهيئة معينة لأمن المعلومات • نتائج وتقارير معينة لعملية التدقيق. • محاضر اللجنة التنفيذية. • تفاصيل المصادقة أو التعريف والتحقق (ID&V) - العميل/الزبون والزميل. • الأحجام الكبيرة لمعلومات مالكي البطاقات. • توقعات الأرباح أو النتائج المالية السنوية (قبل نشرها للجمهور). • أي بنود يتم تغطيتها بموجب اتفاقية رسمية لعدم الإفصاح عن المعلومات (NDA).
مقيدة - داخلية	يجب تصنيف المعلومات على أنها "مقيدة - داخلية" إذا كان المستلمون المتوقعون فقط من موظفي بنك باركليز المصرح لهم وموفري خدمات بنك باركليز المدارة (MSP) الذين لديهم عقد فعال، والتي يقتصر الاطلاع عليها على جمهور معين. يكون للإفصاح عن المعلومات غير المصرح به أثر عكسي على بنك باركليز، والذي يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "جسيم" أو "محدود" (من الناحية المالية أو غير المالية). الهدف من هذه المعلومات ليس التوزيع العام ولكن يمكن توجيهها أو مشاركتها بواسطة المستلمين وفقًا لمبدأ "الحاجة إلى المعرفة".	• الإستراتيجيات والميزانيات. • تقييمات الأداء. • رواتب الموظفين وبياناتهم الشخصية. • تقديرات الثغرات الأمنية. • نتائج وتقارير عملية التدقيق.

مقيدة - خارجية	يجب تصنيف المعلومات على أنها "مقيدة - خارجية" إذا كان المستلمون المتوقعون فقط من موظفي بنك باركليز المصرح لهم وموفري خدمات بنك باركليز MSP الذين لديهم عقد فعال، والتي يقتصر الاطلاع عليها على جمهور معين أو أطراف خارجية يتم التصريح بها بواسطة مالك المعلومات. يكون للإفصاح عن المعلومات غير المصرح به أثر عكسي على بنك باركليز، والذي يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "جسيم" أو "محدود" (من الناحية المالية أو غير المالية). الهدف من هذه المعلومات ليس التوزيع العام ولكن يمكن توجيهها أو مشاركتها بواسطة المستلمين وفقًا لمبدأ "الحاجة إلى المعرفة".	• خطط منتجات جديدة. • عقود العملاء. • العقود القانونية. • معلومات العملاء الفردية/صغيرة الحجم والمستهدف إرسالها إلى أطراف خارجية. • الاتصالات بالعملاء/الزبائن. • مواد عرض إصدار جديد (مثل نشرة اكتتاب ومذكرة عرض). • مستندات الأبحاث النهائية. • المواد غير المتعلقة ببنك باركليز، والمعلومات غير العامة (MNPI). • جميع تقارير الأبحاث • مواد تسويقية معينة. • تعقيبات السوق.
غير مقيدة	معلومات الهدف منها إما التوزيع العام أو التي ليس لها أي تأثير على المؤسسة في حالة توزيعها.	• المواد التسويقية. • المنشورات. • الإعلانات العامة. • إعلانات الوظائف. • معلومات ليس لها تأثير على بنك باركليز.

الجدول ب2: مخطط التعريف بمعلومات بنك باركليز - متطلبات التعامل مع المعلومات

***** تصنيف المعلومات ونتائج التدقيق والسجلات الشخصية التي تتعلق بتهيئة أمن الأنظمة على أنها إما "مقيدة - داخلية" أو "سرية"، ويتوقف هذا على أثر الإفصاح عن الأعمال غير المصرح به**

مراحل دورة الحياة	مقيدة - داخلية	مقيدة - خارجية	سرية
الإعداد والتقديم	• يحق لمالك المعلومات فقط أن يطلع على الأصول.	• يحق لمالك المعلومات فقط أن يطلع على الأصول.	• يحق لمالك المعلومات فقط أن يطلع على الأصول.
التخزين	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة (تشمل أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم). • لا يتعين أن تُترك المعلومات في أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم.	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. • يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مصرح لهم بذلك.	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. • يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مصرح لهم بذلك.

			• جميع المفاتيح الخاصة المستخدمة لحماية بيانات وهوية و/أو سمعة بنك باركليز يجب حمايتها باستخدام وحدات أمن الأجهزة المعتمدة (HSM) من النوع FIPS 140-2، المستوى 3 أو أحدث.
الوصول والاستخدام	• لا يتعين أن تُترك الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة تقع خارج المرافق. • لا يتعين أن تُترك الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسب إذا تطلب الأمر ذلك	• لا يتعين العمل على الأصول (سواء كانت ورقية أو إلكترونية) أو تركها دون رقابة بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها.إلا أنه يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل شاشات الخصوصية). • يجب جمع الأصول المطبوعة من الطابعة على الفور.وفي حال عدم التمكن من ذلك، يلزم الاستعانة بأدوات الطباعة الآمنة. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة.	• لا يتعين العمل على الأصول (سواء كانت ورقية أو إلكترونية) أو تركها دون رقابة بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها.إلا أنه يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل شاشات الخصوصية). • يتعين طباعة الأصول من خلال استخدام أدوات طباعة آمنة. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة
المشاركة	• يتعين وضع ملصق معلومات واضح على الأصول المطبوعة.كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات. • يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة. • يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي.	• يتعين إرفاق ملصق معلومات واضح بالأصول المطبوعة.كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين إرفاق ملصق معلومات واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات.كما يتعين وجود ملصق المعلومات هذا على كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات. • يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة. • يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي. • يجب أن يقتصر توزيع الأصول على الأفراد ممن لديهم أعمال تتطلب ذلك. • لا يتعين إرسال الأصول عن طريق الفاكس باستثناء الحالة التي يكون فيها المرسل على ثقة من أن المرسل إليهم على استعداد لأن يُعيدوا هذه الأصول. • يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية.	• يتعين إرفاق ملصق معلومات واضح على كل صفحة من صفحات الأصول المطبوعة. • يتعين إرفاق ملصق معلومات واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة ويجب إغلاقها بختم ضد العبث.كما يتعين وضع هذه الأصول داخل مغلف ثانوي غير موسوم وذلك قبل توزيعه. • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات.كما يتعين وجود ملصق المعلومات هذا على كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات. • يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة. • يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي. • يجب أن يقتصر توزيع الأصول على الأفراد المخولين بشكل خاص من قبل مالك المعلومات لاستلامها. • ينبغي عدم إرسال الأصول بالفاكس. • يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية. • ينبغي الحفاظ على تسلسل العهدة فيما يتعلق بالأصول الإلكترونية.

الحفظ والإتلاف	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد.	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد. • يتعين حذف أية بيانات موجودة على الوسائط التي يتم تخزين الأصول الإلكترونية السرية عليها بشكل مناسب وذلك قبل أو أثناء عملية التخلص من هذه الوسائط.

الملحق ج: المساحة المخصصة للبنك (BDS)– متطلبات الرقابة (ملاحظة: يرجى مراجعة ممثل توفير الموارد الخاص بك عند اللزوم)

مجال الرقابة	نطاق الرقابة	وصف الرقابة
مساحة مخصصة للبنك	الفصل المادي	المساحة الفعلية التي يتم شغلها يجب تخصيصها لبنك باركليز وعدم مشاركتها مع الشركات/ الموردين الآخرين.
مساحة مخصصة للبنك	مراقبة الوصول المادي	يجب تشغيل الضوابط التلقائية للأمن من أجل الوصول إلى المساحة المخصصة للبنك وتشمل: 1) بالنسبة للموظفين المصرح لهم: أ) بطاقة تعريف مصحوبة بصورة ظاهرة في جميع الأوقات ب) استخدام أجهزة لقراءة البطاقات عن قرب ج) تمكين آلية لمنع تمرير بيانات الاعتماد لأشخاص آخرين 2) ضوابط الزوار/الموردين أ) الدخول إلى دفتر التسجيل أ) بطاقة تعريف للاستخدام المحدود ظاهرة في جميع الأوقات
مساحة مخصصة للبنك	مراقبة الوصول المادي	يجب تهيئة الإنذارات للإبلاغ من خلال نظام مركزي للوصول مع تحكم في الوصول قابل للتحقق
مساحة مخصصة للبنك	مراقبة الوصول المادي وأعمال الصيانة	مراقبة الضوابط التي تضمن منح الوصول المناسب إلى المساحة المخصصة للبنك والمناطق الحيوية الأخرى يتم السماح بتواجد أفراد معينين فقط في المساحة المخصصة للبنك ويشمل هذا موظفي الدعم وأعمال الصيانة المصرح لهم بذلك مثل فني الكهرباء وعمال الصيانة وغيرهم
مساحة مخصصة للبنك	الوصول عن بعد - المصادقة أو التعريف والتحقق	يجب أن تتم المصادقة على دخول كل مستخدم مفرد لشبكة بنك باركليز فقط من المساحة المخصصة للبنك باستخدام الرمز المميز للمصادقة متعددة العوامل الذي يوفره البنك

مساحة مخصصة للبنك	الوصول عن بعد - الرموز المميزة للبرامج	يجب أن يتم تثبيت أي برامج لخوارزميات التشفير RSA والرموز المميزة البرمجية بواسطة موظف مصرح له بذلك داخل المساحة المخصصة للبنك المتفق عليها على أسطح المكتب
مساحة مخصصة للبنك	الوصول عن بعد - الدعم أثناء التواجد خارج المكاتب	لا يتم توفير الوصول عن بعد للمساحة المخصصة للبنك بطريقة افتراضية بهدف دعم العمل في غير ساعات الدوام أو أثناء التواجد خارج المكاتب.يجب الحصول على الموافقة على أي اتصال عن بُعد بواسطة فرق بنك باركليز ذات الصلة (ويشمل ذلك كبير المسؤولين عن الأمن)
مساحة مخصصة للبنك	البريد الإلكتروني والإنترنت	يجب تهيئة الاتصالات بالشبكة بطريقة آمنة تمنع أنشطة البريد الإلكتروني والإنترنت على شبكة المساحة المخصصة للبنك
مساحة مخصصة للبنك	تطوير البرامج، والاختبار، وبيئة التطوير	يتعين على المورد التأكد من أن تطوير البرامج يتم فقط من أجل البرامج التي يملكها بنك باركليز داخل المساحة المخصصة للبنك.
مساحة مخصصة للبنك	ضوابط الشبكة - النقل	يجب نقل جميع المعلومات بطريقة آمنة بين بيئة المساحة المخصصة للبنك وبنك باركليز، وأن تتم إدارة أجهزة الشبكة باستخدام بروتوكولات اتصالات آمنة
مساحة مخصصة للبنك	ضوابط الشبكة - التوجيه	يجب ضمان أن التهيئة تقوم بإعادة توجيه الاتصالات إلى شبكة بنك باركليز فقط ويجب ألا تعيد التوجيه إلى أي شبكات أخرى
مساحة مخصصة للبنك	ضوابط الشبكة - الاتصالات اللاسلكية	يجب عدم استخدام الشبكات اللاسلكية في شبكة بنك باركليز الخاصة بقطاع توفير الخدمات.

سرية التعاملات البنكية

ضوابط إضافية للاختصاصات القضائية المتعلقة بسرية التعاملات البنكية في سويسرا وموناكو فقط

مجال / نطاق الرقابه	وصف الرقابه	الاهميه
1. الأدوار والمسؤوليات	يجب على المورد تحديد الأدوار والمسؤوليات الخاصة بالتعامل مع بيانات تعريف العميل (والتي سيتم الإشارة إليها فيما يلي بالاختصار CID) وتوصيلها إلى الموظفين.يتعين على المورد مراجعة المستندات التي توضح الأدوار والمسؤوليات المتعلقة ببيانات تعريف العميل بعد أي تغيير مادي على النموذج التشغيلي للمورد (أو نموذج الأعمال) أو مرة واحدة على الأقل سنويًا وتوزيعها على الاختصاص القضائي لسرية التعاملات البنكية ذي الصلة ينبغي أن تشمل الأدوار الرئيسية أحد كبار المسؤولين التنفيذيين ليتولى حماية والإشراف على جميع الأنشطة المتعلقة ببيانات تعريف العميل (يرجى الرجوع إلى الملحق "أ" للاطلاع على معنى بيانات تعريف العميل)	تعريف واضح للأدوار والمسؤوليات التي تدعم تطبيق جدول التزامات الرقابة على المورد الخارجي.
2. الإبلاغ عن انتهاك بيانات تعريف العميل	يجب تطبيق الضوابط والعمليات الموثقة لضمان الإبلاغ عن أي انتهاكات تؤثر على بيانات تعريف العميل والتعامل معها. أي انتهاك لمتطلبات التعامل (كما هو منصوص عليه في الجدول ب2) يجب أن يرد المورد عليه والإبلاغ عنه إلى الاختصاص القضائي لسرية التعاملات البنكية ذي الصلة على الفور (خلال 24 ساعة على الأقل).يتعين اتباع عملية استجابة للحوادث فيما يتعلق بالأحداث التي تتضمن التعامل مع بيانات تعريف العميل والإبلاغ عنها بصفة دورية في الوقت المناسب. يتعين على المورد ضمان اتباع الإجراءات التصحيحية المحددة بعد وقوع حادث من خلال وضع خطة للإصلاح (تشمل الإجراء والملكية وتاريخ التنفيذ) ومشاركتها مع الاختصاص القضائي لسرية التعاملات البنكية ذي الصلة واعتمادها من جانبه.	تساعد عملية الاستجابة للحادثة على التأكد من احتواء الحوادث بسرعة ومنع تصاعد خطورتها. أي انتهاك يؤثر على بيانات تعريف العميل يمكن أن يؤدي إلى إضرار كبير بالسمعة أو أضرار لبنك باركليز ويمكن أن تؤدي إلى توقيع غرامات وفقدان ترخيص مزاولة التعاملات البنكية في سويسرا أو موناكو
3. التثقيف والتوعية	يتعين على موظفي المورد الذين يملكون حق الوصول إلىبيانات تعريف العميل و/أو يتعاملون معها يجب عليهم حضور التدريب* الذي يطبق متطلبات سرية التعاملات البنكية الخاصة ببيانات تعريف العميل بعد أي تغيير جديد على اللوائح التنظيمية أو مرة واحدة على الأقل في السنة. يتعين على المورد التأكد من أن جميع الموظفين الجدد لديه (الذين يملكون حق الوصول إلى بيانات تعريف العميل و/أو يتعاملون معها)، خلال فترة زمنية معقولة (حوالي 3 شهور)، يجب عليهم حضور التدريب الذي يضمن فهم مسؤولياتهم المتعلقة ببيانات تعريف العميل. يتعين على المورد الاحتفاظ بسجل للموظفين الذين أكملوا التدريب. * ستقوم الاختصاصات القضائية لسرية التعاملات البنكية بتوفير توجيهات بشأن المحتوى المتوقع وجوده في مواد التدريب.	تدعم عملية التثقيف والتوعية جميع الضوابط الأخرى الموجودة في هذا الجدول.

4. مخطط تعريف المعلومات	**عند اللزوم***، يجب على المورد تطبيق مخطط تعريف معلومات بنك باركليز (الجدول د1 في الملحق د)، أو مخطط بديل متفق عليه مع الاختصاص القضائي لسرية التعاملات البنكية، على جميع أصول المعلومات التي يتم الاحتفاظ بها أو معالجتها بالنيابة عن الاختصاص القضائي لسرية التعاملات البنكية. متطلبات التعامل مع بيانات تعريف العميل موجودة في الجدول د2 في الملحق د. * **"عند اللزوم"** يشير إلى فوائد التعريف بالمعلومات مع ضرورة إحداث توازن مع التكلفة المتضمنة. على سبيل المثال، يعد تعريف مستند ما أمرًا غير مناسبًا، حال كان ذلك مخالفًا للمتطلبات التنظيمية لمكافحة التزوير والتلاعب.	تعد قائمة المخزون الكاملة والدقيقة لأصول المعلومات أمرًا ضروريًا للتأكد من استخدام الضوابط المناسبة.
5. الحوسبة السحابية/التخزين الخارجي	جميع استخدامات الحوسبة السحابية و/أو التخزين الخارجي لبيانات تعريف العميل (في خوادم موجودة خارج الاختصاص القضائي لسرية التعاملات البنكية وبعيدًا عن البنية التحتية للمورد) التي يتم الاستفادة منها كجزء من الخدمات لذلك الاختصاص القضائي يجب الموافقة عليه من قبل الفرق المحلية المقابلة ذات الصلة (وتشمل كبير المسؤولين عن الأمن، والالتزام والشؤون القانونية)؛ ويجب تطبيق الضوابط بما يتماشى مع الاختصاص القضائي لسرية التعاملات البنكية للحماية من نقص المعلومات الخاصة ببيانات تعريف العميل فيما يتعلق بحجم المخاطر المرتفعة التي تمثلها.	في حال عدم تطبيق هذا المبدأ، يمكن أن تتعرض بيانات العملاء (بيانات تعريف العميل) المحمية بطريقة غير مناسبة للخطر مما قد يؤدي إلى توقيع عقوبات قانونية وتنظيمية أو الإضرار بالسمعة.

** بيانات تعريف العميل هي بيانات خاصة وفقًا لقوانين سرية التعاملات البنكية المطبقة في سويسرا وموناكو. وبالتالي، تكون الضوابط المدرجة هنا مكملة لتلك الضوابط المذكورة أعلاه.

المصطلح	التعريف
CID	بيانات تعريف العميل
CIS	الأمن الإلكتروني وأمن المعلومات

موظف المورد	أي شخص تم تعيينه مباشرةً مع المورد كموظف دائم أو أي فرد يوفر خدمات إلى المورد خلال فترة زمنية محدودة (مثل الاستشاري)
الأصل	أي جزء منفرد من المعلومات أو تجميع للمعلومات له قيمة
نظام	النظام، في سياق هذا المستند، عبارة عن أشخاص وإجراءات ومعدات وبرامج تكنولوجيا المعلومات.يتم استخدام عناصر هذا الكيان المركب معًا في البيئة التشغيلية أو بيئة الدعم المستهدفة لأداء مهمة معينة أو تحقيق غرض معين أو دعم أو متطلبات خاصة بإحدى المهام.
مستخدم	حساب مخصص لأحد موظفي المورد أو الاستشاري أو المقاول أو عامل الوكالة الذي يملك حق الوصول المصرح به للنظام الذي يمتلكه بنك باركليز دون تمتعه بأي امتيازات عالية المستوى.

الملحق د:معنى "بيانات تعريف العميل"

بيانات تعريف العميل المباشرة (DCID) يمكن تعريفها على أنها معرفات فريدة (يمتلكها العميل)، والتي تسمح كما هي وبنفسها، لتعريف عميل دون الوصول إلى البيانات الموجودة في تطبيقات التعاملات البنكية الخاصة ببنك باركليز.يجب أن تكون هذه البيانات غير غامضة ولا تخضع للتأويل ويمكن أن تشمل معلومات مثل الاسم واسم العائلة واسم الشركة والتوقيع وهوية الشبكة الاجتماعية وغيرها. تشير بيانات تعريف العميل المباشرة إلى بيانات العميل التي لا يمتلكها البنك أو لم يقم بإنشائها.

بيانات تعريف العميل غير المباشرة (ICID) مقسمة إلى 3 مستويات

- **بيانات تعريف العميل غير المباشرة - المستوى 1** تشير إلى معرفات فريدة (يملكها البنك) والتي تسمح بتعريف عميل بشكل فريد في حال توفير الوصول إلى تطبيقات التعاملات البنكية أو تطبيقات الأطراف **الخارجية الأخرى**. يجب أن يكون هذا المعرف غير غامض ولا يخضع للتأويل ويمكن أن يشمل معرفات مثل رقم الحساب ورمز معرف الحساب الدولي، ورقم بطاقة الائتمان وغيرها.

- **بيانات تعريف العميل غير المباشرة - المستوى 2** تشير إلى معلومات (يملكها العميل)، والتي يمكن مع معلومات أخرى أن تؤدي لاستنتاج هوية عميل.وعلى الرغم من أنه لا يمكن استخدام هذه المعلومات بمفردها لتعريف عميل، فإنه يمكن استخدامها مع معلومات أخرى لتعريف عميل.يجب حماية بيانات تعريف العميل غير المباشرة من المستوى 2 وإدارتها بنفس صرامة بيانات تعريف العميل المباشرة.

- **بيانات تعريف العميل غير المباشرة - المستوى 3** تشير إلى معرفات فريدة ولكنها مجهولة الهوية (يملكها البنك) والتي تسمح بتعريف عميل في حال توفير الوصول إلى تطبيقات التعاملات البنكية.الفارق بالمقارنة مع بيانات تعريف العميل غير المباشرة من المستوى 1 هو أن تصنيف المعلومات يكون "مقيدة - خارجية" بدلاً من سرية التعاملات البنكية، وهو ما يعني أنها لن تخضع لنفس الضوابط.

يرجى الرجوع إلى الشكل رقم 1 الخاص بهيكل قرار بيانات تعريف العميل للحصول على نظرة عامة على أسلوب التصنيف.

يجب عدم مشاركة بيانات تعريف العميل غير المباشرة من المستوى 1 مع أي شخص موجود خارج البنك ويجب احترام مبدأ "الحاجة إلى المعرفة" في جميع الأوقات.يمكن مشاركة بيانات تعريف العميل غير المباشرة من المستوى 2 على أساس مبدأ "الحاجة إلى المعرفة" ولكن لا يمكن مشاركتها مع أي أجزاء أخرى من بيانات تعريف العميل.عن طريق مشاركة أجزاء متعددة من بيانات تعريف العميل، توجد احتمالية لتكوين "مزيج سام" والذي من المحتمل أن يؤدي للكشف عن هوية أحد العملاء.ونحن نعرّف المزيج السام على أنه يبدأ بجزأين من بيانات تعريف العميل غير المباشرة من المستوى 2 على الأقل.يمكن مشاركة بيانات تعريف العميل غير المباشرة من المستوى 3 غير المصنفة ضمن معلومات مستوى سرية التعاملات البنكية، وذلك ما لم يؤدي الاستخدام المتكرر لنفس المعرف إلى جمع بيانات لتعريف العميل غير المباشرة من المستوى 2 كافية للكشف عن هوية العميل.

تصنيف المعلومات	سرية التعاملات البنكية		مقيدة - داخلية
التصنيف	**بيانات تعريف العميل المباشرة (DCID)**	**بيانات تعريف العميل غير المباشرة (ICID)**	
		غير مباشرة (المستوى 1)	**غير مباشرة محتملة (المستوى 2)**	**معرف غير شخصي (المستوى 3)**
نوع المعلومات	اسم العميل	رقم الحاوية/ هوية الحاوية	الاسم	هوية المعالجة الداخلية
	اسم الشركة	رقم MACC (حساب أموال، بموجب هوية حاوية Avaloq)	تاريخ الميلاد	المعرف الفريد الثابت
	بيان الحساب	العنوان	الجنسية	المعرف الديناميكي
	التوقيع	رمز معرف الحساب الدولي	النطاق	هوية الحاوية الخارجية

هوية الشبكة الاجتماعية	تفاصيل الدخول إلى التعاملات البنكية الإلكترونية	وضع الأسرة	
رقم جواز السفر	رقم حفظ الودائع	الرمز البريدي	
رقم الهاتف	رقم بطاقة الائتمان	وضع الثروة	
عنوان البريد الإلكتروني		اسم العائلة	
المسمى الوظيفي		آخر زيارة للعميل	
اسم الفنان		اللغة	
عنوان IP		النوع	
رقم الفاكس		تاريخ انتهاء بطاقة الائتمان	
		مسؤول الاتصال الأساسي	
		مكان الميلاد	
		تاريخ فتح الحساب	
		قيمة الوضع/المعاملة الكبيرة	

مثال: إذا قمت بإرسال بريد إلكتروني أو شاركت أي مستند مع أشخاص خارجيين (يشمل هذا الأطراف الخارجية في سويسرا/موناكو) أو الزملاء في العمل داخل المؤسسة مع شريك/شركة تابعة موجودة في سويسرا/موناكو أو بلدان أخرى (مثل المملكة المتحدة)

1. اسم العميل

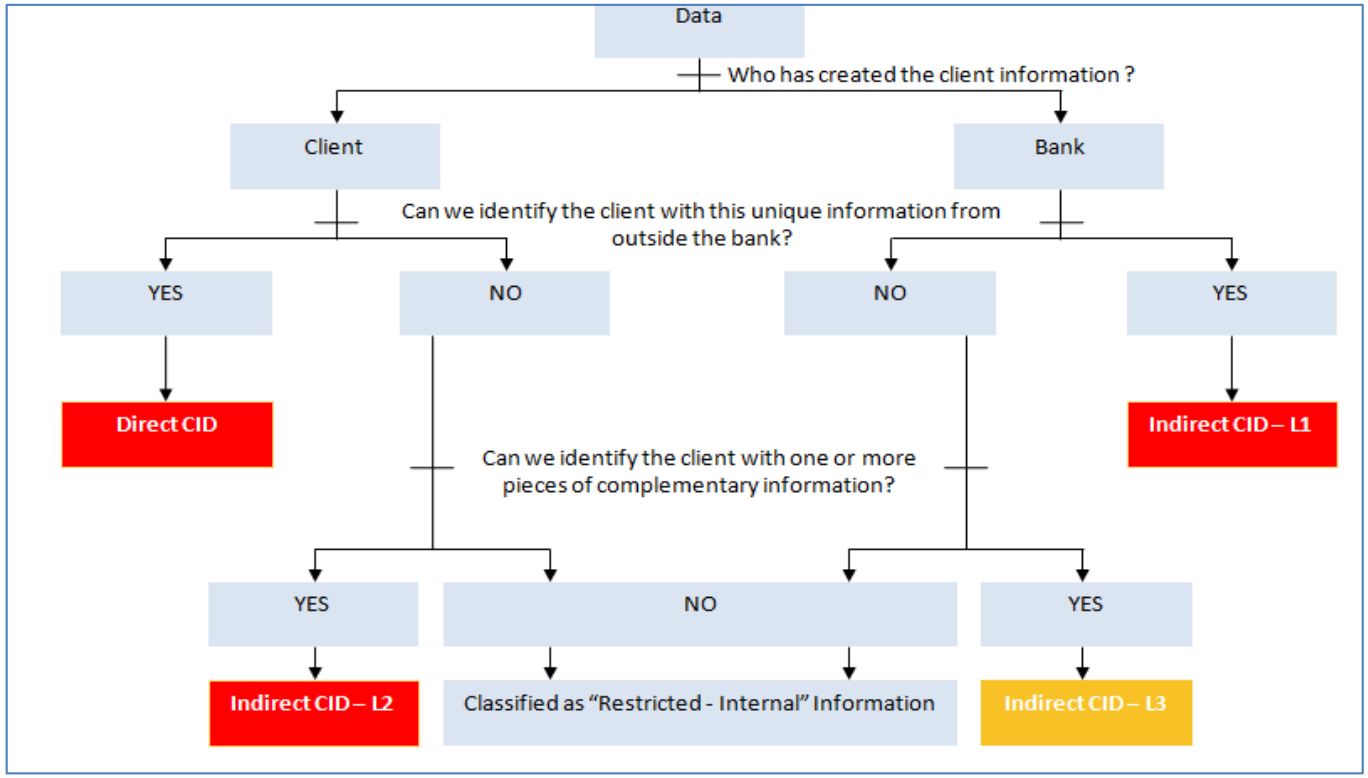
(بيانات تعريف العميل المباشرة) = انتهاك لسرية التعاملات البنكية

2. هوية الحاوية

(بيانات تعريف العميل غير المباشرة - المستوى 1) = انتهاك لسرية التعاملات البنكية

3. وضع الثروة + الجنسية

(بيانات تعريف العميل غير المباشرة - المستوى 2) + (بيانات تعريف العميل غير المباشرة - المستوى 2) = انتهاك لسرية التعاملات البنكية



المخطط هـ:مخطط تعريف معلومات بنك باركليز

الجدول هـ 1:مخطط تعريف معلومات بنك باركليز

** "سرية التعاملات البنكية" هو تعريف خاص بالاختصاصات القضائية لسرية التعاملات البنكية.

الملصق	التعريف	الأمثلة
سرية التعاملات البنكية	المعلومات المرتبطة بأي بيانات تعريف للعميل (CID) سواء كانت سويسرية أو مباشرة أو غير مباشرة. ينطبق تصنيف "سرية التعاملات البنكية" على المعلومات المرتبطة بأي بيانات تعريف للعميل (CID) سواء كانت مباشرة أو غير مباشرة.ولذلك، يكون وصول جميع الموظفين، بما فيهم الموجودين في الاختصاص القضائي المالك للمعلومات، غير ملائم. يكون الوصول إلى هذه المعلومات مطلوبًا فقط من قبل هؤلاء الذين لديهم حاجة إلى المعرفة لإنجاز واجباتهم الرسمية أو مسؤولياتهم التعاقدية. قد يكون للإفصاح غير المصرح به عن كيان هذه المعلومات أو الوصول إليها أو مشاركتها داخليًا أو خارجيًا أثرًا خطيرًا، وقد يؤدي إلى دعاوى جنائية وله عواقب مدنية وإدارية مثل توقيع الغرامات وفقدان ترخيص مزاولة التعاملات البنكية، إذا تم الإفصاح عنها لموظفين غير مصرح لهم بذلك سواء على المستوى الداخلي أو الخارجي.	• اسم العميل • عنوان العميل • التوقيع • عنوان IP الخاص بالعميل (توجد أمثلة إضافية في الملحق)

الملصق	التعريف	الأمثلة
سرية	يجب تصنيف المعلومات على أنها "سرية" إذا كان الكشف عنها غير المصرح به سيؤدي إلى أثر عكسي على بنك باركليز يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "حرج" (من الناحية المالية أو غير المالية). يتم تقييد هذه المعلومات لتصبح متاحة لجمهور معين فقط ولا يجب توزيعها إلى أي شخص آخر دون الحصول إلى إذن من المُنشئ.قد يشمل الجمهور مستلمين خارجيين بناء على تفويض صريح من مالك المعلومات.	• معلومات حول عمليات الدمج أو الاستحواذ المحتملة. • معلومات التخطيط الإستراتيجي - الخاصة بالأعمال والمعلومات التنظيمية. • معلومات محددة خاصة بتهيئة الأمن. • نتائج وتقارير معينة لعملية التدقيق. • محاضر اللجنة التنفيذية. • تفاصيل المصادقة أو التعريف والتحقق (ID&V) - العميل/الزبون والزميل. • الأحجام الكبيرة لمعلومات مالكي البطاقات. • توقعات الأرباح أو النتائج المالية السنوية (قبل نشرها للجمهور). • أي بنود يتم تغطيتها بموجب اتفاقية رسمية لعدم الإفصاح عن المعلومات (NDA).
مقيدة - داخلية	يجب تصنيف المعلومات على أنها "مقيدة - داخلية" إذا كان المستلمون المتوقعون فقط من موظفي بنك باركليز المصرح لهم وموفري خدمات بنك باركليز المدارة (MSP) الذين لديهم عقد فعال، والتي يقتصر الاطلاع عليها على جمهور معين.	• الإستراتيجيات والميزانيات. • تقييمات الأداء. • رواتب الموظفين وبياناتهم الشخصية. • تقديرات الثغرات الأمنية. • نتائج وتقارير عملية التدقيق.

	يكون للإفصاح عن المعلومات غير المصرح به أثر عكسي على بنك باركليز، والذي يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "جسيم" أو "محدود" (من الناحية المالية أو غير المالية). الهدف من هذه المعلومات ليس التوزيع العام ولكن يمكن توجيهها أو مشاركتها بواسطة المستلمين وفقًا لمبدأ "الحاجة إلى المعرفة".	
مقيدة - خارجية	يجب تصنيف المعلومات على أنها "مقيدة - خارجية" إذا كان المستلمون المتوقعون فقط من موظفي بنك باركليز المصرح لهم وموفري خدمات بنك باركليز MSP الذين لديهم عقد فعال، والتي يقتصر الاطلاع عليها على جمهور معين أو أطراف خارجية يتم التصريح بها بواسطة مالك المعلومات. يكون للإفصاح عن المعلومات غير المصرح به أثر عكسي على بنك باركليز، والذي يتم تقديره بموجب "إطار عمل إدارة مخاطر المؤسسة" (ERMF) على أنه "جسيم" أو "محدود" (من الناحية المالية أو غير المالية). الهدف من هذه المعلومات ليس التوزيع العام ولكن يمكن توجيهها أو مشاركتها بواسطة المستلمين وفقًا لمبدأ "الحاجة إلى المعرفة".	• خطط منتجات جديدة. • عقود العملاء. • العقود القانونية. • معلومات العملاء الفردية/صغيرة الحجم والمستهدف إرسالها إلى أطراف خارجية. • الاتصالات بالعملاء/الزبائن. • مواد عرض إصدار جديد (مثل نشرة اكتتاب ومذكرة عرض). • مستندات الأبحاث النهائية. • المواد غير المتعلقة ببنك باركليز، والمعلومات غير العامة (MNPI). • جميع تقارير الأبحاث • مواد تسويقية معينة. • تعقيبات السوق.
غير مقيدة	معلومات الهدف منها إما التوزيع العام أو التي ليس لها أي تأثير على المؤسسة في حالة توزيعها.	• المواد التسويقية. • المنشورات. • الإعلانات العامة. • إعلانات الوظائف. • معلومات ليس لها تأثير على بنك باركليز.

الجدول هـ 2: مخطط التعريف بالمعلومات - متطلبات التعامل مع المعلومات

** متطلبات خاصة للتعامل مع بيانات تعريف العميل للتأكد من سريتها بما يتماشى مع المتطلبات التنظيمية

مراحل دورة الحياة	متطلبات سرية التعاملات البنكية
الإنشاء والتعريف	وفقًا للفئة "مقيدة - خارجية) و: • يجيب تخصيص مالك لبيانات تعريف العميل.

التخزين	وفقًا للفئة "مقيدة - خارجية) و: • يتعين تخزين الأصول على وسائط قابلة للإزالة فقط طالما كان ذلك مطلوبًا بصورة صريحة لسد احتياجات معينة للأعمال أو المنظمين أو المدققين الخارجيين. • يجب عدم تخزين أحجام كبيرة من أصول معلومات سرية التعاملات البنكية على جهاز/وسائط محمولة. لمعرفة مزيد من المعلومات، اتصل بالفريق المحلي المختص بالأمن الإلكتروني وأمن المعلومات (واختصاره CIS). • لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مصرح لهم إلى هذه الأصول أو اطلاعهم عليها، وفقًا لمبدأ "الحاجة إلى المعرفة" أو "الحاجة إلى الحصول". • يجب اتباع ممارسات مكان العمل الآمن مثل سطح المكتب المنظم وتأمين شاشة الكمبيوتر للاحتفاظ بالأصول (سواء كانت مادية أو إلكترونية) بطريقة آمنة. • يجب استخدام الوسائط القابلة للإزالة لتخزين أصول المعلومات فقط إذا كان هذا الأمر مطلوبًا بطريقة صريحة، مع قفلها وتأمينها أثناء عدم الاستخدام. • تتطلب عمليات نقل البيانات حسب الحاجة إلى أجهزة/وسائط محمولة الحصول على موافقة مالك البيانات وفرق الالتزام والأمن الإلكتروني وأمن المعلومات.
الوصول والاستخدام	وفقًا للفئة "مقيدة - خارجية) و: • لا يجب إزالة الأصول أو عرضها بعيدًا عن الموقع (منشآت بنك باركليز) دون الحصول على مصادقة رسمية من مالك بيانات تعريف العميل (أو نائبه). • لا يجب إزالة الأصول أو عرضها بعيدًا عن الاختصاص القضائي للاحتفاظ بدفاتر العملاء دون الحصول على مصادقة رسمية من مالك بيانات تعريف العميل (أو نائبه)، والعميل (تنازل اختياري/ تفويض رسمي محدود). • يجب اتباع الممارسات الآمنة للعمل عن بُعد، والتي تضمن عدم السماح "بقراءة رمز مستعمل عن طريق التلصص"، عند أخذ الأصول المادية بعيدًا عن الموقع.
	• تأكد من عدم قدرة الأشخاص غير المصرح لهم على مراقبة أو الوصول إلى الأصول الإلكترونية التي تتضمن بيانات تعريف العميل من خلال استخدام الوصول المقيد إلى تطبيقات الأعمال.
المشاركة	وفقًا للفئة "مقيدة - خارجية) و: • يجب أن يقتصر توزيع الأصول على "مبدأ الحاجة إلى المعرفة" فقط، وداخل أنظمة وفرق عمل معلومات الاختصاص القضائي لسرية التعاملات البنكية الخاص بالمنشئ. • تحتاج الأصول التي يتم نقلها حسب الحاجة باستخدام وسائط محمولة للحصول على موافقة مالك أصول المعلومات وفرق الأمن الإلكتروني وأمن المعلومات. • يتعين تشفير الاتصالات الإلكترونية أثناء إرسالها. • يجب تسليم الأصول (النسخة المطبوعة) المرسلة بواسطة البريد العادي عن طريق خدمة تطلب الحصول على إيصال بتأكيد الاستلام. • يجب أن يتم توزيع الأصول وفقًا "لمبدأ الحاجة إلى المعرفة" فقط.
الأرشفة والتخلص	وفقًا للفئة "مقيدة - خارجية)

*** تصنيف المعلومات ونتائج التدقيق والسجلات الشخصية التي تتعلق بتهيئة أمن الأنظمة على أنها إما "مقيدة - داخلية" أو "سرية"، ويتوقف هذا على أثر الإفصاح عن الأعمال غير المصرح به

مراحل دورة الحياة	مقيدة - داخلية	مقيدة - خارجية	سرية
الإعداد والتقديم	• يحق لمالك المعلومات فقط أن يطلع على الأصول.	• يحق لمالك المعلومات فقط أن يطلع على الأصول.	• يحق لمالك المعلومات فقط أن يطلع على الأصول.
التخزين	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة (تشمل أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم). • لا يتعين أن تُترك المعلومات في أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم.	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. • يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مصرح لهم بذلك.	• لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. • يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مصرح لهم بذلك. • جميع المفاتيح الخاصة المستخدمة لحماية بيانات وهوية و/أو سمعة بنك باركليز يجب حمايتها باستخدام وحدات أمن الأجهزة المعتمدة (HSM) من النوع FIPS 140-2، المستوى 3 أو أحدث.
الوصول والاستخدام	• لا يتعين أن تُترك الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة تقع خارج المرافق. • لا يتعين أن تُترك الأصول (سواء كانت ورقية أو إلكترونية) في أماكن عامة تقع داخل المرافق مما يسمح للزائرين بالوصول إليها دون وجود إشراف عليهم. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسب إذا تطلب الأمر ذلك	• لا يتعين العمل على الأصول (سواء كانت ورقية أو إلكترونية) أو تركها دون رقابة بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. إلا أنه يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل شاشات الخصوصية). • يجب جمع الأصول المطبوعة من الطابعة على الفور. وفي حال عدم التمكن من ذلك، يلزم الاستعانة بأدوات الطباعة الآمنة. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة.	• لا يتعين العمل على الأصول (سواء كانت ورقية أو إلكترونية) أو تركها دون رقابة بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها. إلا أنه يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل شاشات الخصوصية). • يتعين طباعة الأصول من خلال استخدام أدوات طباعة آمنة. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة
المشاركة	• يتعين وضع ملصق معلومات واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات. • يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة. • يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي.	• يتعين إرفاق ملصق معلومات واضح بالأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين إرفاق ملصق معلومات واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات. كما يتعين وجود ملصق المعلومات هذا على كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات. • يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة.	• يتعين إرفاق ملصق معلومات واضح على كل صفحة من صفحات الأصول المطبوعة. • يتعين إرفاق ملصق معلومات واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة ويجب إغلاقها بختم ضد العبث. كما يتعين وضع هذه الأصول داخل مغلف ثانوي غير موسوم وذلك قبل توزيعه. • يتعين أن تحتوي الأصول الإلكترونية على ملصق واضح للتعريف بالمعلومات. كما يتعين وجود ملصق المعلومات هذا على كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات.

		• يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي. • يجب أن يقتصر توزيع الأصول على الأفراد ممن لديهم أعمال تتطلب ذلك. • لا يتعين إرسال الأصول عن طريق الفاكس باستثناء الحالة التي يكون فيها المرسل على ثقة من أن المرسل إليهم على استعداد لأن يُعيدوا هذه الأصول. • يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية.	• يجب أن يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة. • يجب أن يقتصر توزيع الأصول على الموظفين لدى المؤسسة أو على مَن لديهم التزام تعاقدي معها أو كجزء من العمل المعترف به بشكل واضح والذي يتطلب مثل هذا التفاوض التعاقدي. • يجب أن يقتصر توزيع الأصول على الأفراد المخولين بشكل خاص من قبل مالك المعلومات لاستلامها. • ينبغي عدم إرسال الأصول بالفاكس. • يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية. • ينبغي الحفاظ على تسلسل العهدة فيما يتعلق بالأصول الإلكترونية.
الحفظ والإتلاف	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد.	• يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة. • يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد. • يتعين حذف أية بيانات موجودة على الوسائط التي يتم تخزين الأصول الإلكترونية السرية عليها بشكل مناسب وذلك قبل أو أثناء عملية التخلص من هذه الوسائط.