# (SCO) الموردين بمراقبة الالتزام

## متطلبات الرقابة الإدارية للالتزام بمراقبة الموردين

أمن المعلومات، والأمن الإلكتروني والمادي، والتكنولوجيا، وتخطيط الاسترداد، وخصوصية البيانات، وإدارة البيانات، وضوابط EUDA

## MC 1.0 – الحوكمة والقابلية للمساءلة

يجب أن يضع المُورّد إطار عمل معياريًا وثابتًا ومتسقًا لتكنولوجيا المعلومات وأمن تكنولوجيا المعلومات والأمان المادي والتخطيط لاسترداد البيانات بعد الكوارث وإدارة البيانات وحوكمة إدارة المعلومات الشخصية (خصوصية البيانات/حماية البيانات) (حسب معايير NIST، و ISO/IEC 27001، وCOBIT، وBS10012، و18 SSAE، وITIL) أو إطار عمل معياريًا مماثلاً لأفضل الممارسات في القطاع الصناعي لضمان المصادقة على الفعالية التشغيلية لوسائل الحماية أو التدابير المضادة المتبعة في عمليته وبيئته التقنية والمادية. ويجب أن يكفل برنامج الحوكمة الجيد التنظيم والمتبع على نطاق المؤسسة دعم المفاهيم الأساسية المتعلقة بالتوافر والنزاهة والسرية عن طريق الضوابط الملائمة. تجب صياغة الضوابط الرقابية للحدّ من مخاطر فقدان المعلومات أو انقطاعها أو تلفها أو تقليصها، ويجب على المورّد أن يضمن تطبيق ضوابط متطلبات بنك باركليز وتنفيذها بفعالية لحماية الخدمة (الخدمات) التي يتم تقديمها إلى بنك باركليز.

يجب وضع إطار للحوكمة، ويجب أن يتضمن وسائل حماية إدارية وتقنية ومادية لحماية الأصول والمعلومات/البيانات من الفقدان العرضي و/أو المتعمد أو الإفصاح عنها أو تغييرها أو إتلافها أو سرقتها أو استخدامها على نحو غير ملائم أو سوء استخدامها والوصول إليها أو استخدامها أو الإفصاح عنها على نحو غير مصرح به.

يجب أن يتضمن برنامج الحوكمة وقابلية المساءلة، على سبيل المثال لا الحصر، المجالات الآتية:

- سياسات الحوكمة - يجب تعريف مجموعة من السياسات الخاصة بالحوكمة والموافقة عليها من قِبل الإدارة ونشرها وإبلاغها إلى موظفي الموردين والأطراف ذات الصلة والالتزام بها.
  - برامج السياسات والإجراءات والمعايير التي تنشئ السياسات والمعايير بفاعلية، وتقيس الفعالية في تنفيذها باستمرار، وتطبقها.
  - برنامج حوكمة شامل بهيكل واضح للقيادة وإشراف تنفيذي لخلق ثقافة القابلية المساءلة والوعي.
  - التوعية المستمرة بالسياسات والإجراءات المعتمدة عبر مختلف القطاعات المؤسسية.
  - ملاءمة المتطلبات القانونية مع السياسات والممارسات، وحماية البيانات حسب الخطة ووفق الضوابط الأخرى لضمان تنفيذ السياسات والعمليات بفعالية
- مراجعة سياسات الحوكمة وآلياتها وضوابطها ومراقبتها بما يكفل تنفيذ السياسات والعمليات تنفيذًا فعّالاً
- تجب مراجعة السياسات المتبعة في كل المجالات على فترات زمنية مخططة أو في حال حدوث تغييرات بارزة لضمان استمرار ملاءمتها وكفاءتها وفعاليتها.
  - تأكّد من مراجعة السياسات والإجراءات/المعايير بصورة روتينية (على الأقل سنويًا أو عند حدوث أي تغييرات جوهرية، أيهما وقع أولاً).
- الأدوار والمسؤوليات - يجب تحديد المسؤوليات وتوزيعها.
  - قابلية المساءلة الفردية والملكية بخصوص أصول المعلومات
  - تعيين فرد (أفراد) متمرس ومؤهل بشكل مناسب يمكن لبنك باركليز التواصل معه بشأن الأمن المادي وفي المباني، والمعلومات والأمن الإلكتروني وإدارة المعلومات الشخصية (خصوصية البيانات/حماية البيانات) ويكون مسؤولاً عن ضمان تطبيق السياسات والممارسات وحماية البيانات حسب الخطة ووفق الضوابط الأخرى، ومراقبتها بفعالية.
  - يجب على المورّد تنسيق الأدوار والمسؤوليات المنوطة بالموظفين الذين يطبقون الضوابط ويديرونها ويراقبون فعاليتها مع المتعهدين/معالجي البيانات من الباطن الداخليين ومن الباطن وأن يضفي التناغم عليها.
- يجب على المورّد تنفيذ بنية تحتية آمنة وإطار عمل للضوابط المرعية لحماية المؤسسة من أي تهديدات (بما في ذلك الأمن السيبراني)
- المراجعة والتقييمات المستقلة - تجب مراجعة نهج الموردين تجاه إدارة برنامج هندسة أمن المعلومات وتنفيذه (أي أهداف الرقابة والضوابط والسياسات والعمليات والإجراءات المتعلقة بأمن المعلومات) بصورة مستقلة على فترات زمنية مقررة أو عند حدوث تغييرات جوهرية.
  - يجب إجراء المراجعات والتقييمات المستقلة سنويًا على الأقل لضمان معالجة المؤسسة حالات عدم التطابق بين السياسات والمعايير والإجراءات والتزامات الامتثال المعمول بها.
  - تجب مراجعة أنظمة المعلومات سنويًا على الأقل لضمان استمرار التوافق مع سياسات أمن المعلومات في المؤسسة ومعاييرها.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب تعريف سياسة أمن المعلومات للحوسبة السحابية بأنها السياسة الخاصة بالموضوعات التي تسري على عميل خدمة السحابة. يجب أن تكون سياسة أمن المعلومات السارية على عميل خدمة السحابة والخاصة بالحوسبة السحابية متسقة مع المستويات المقبولة لمخاطر أمن المعلومات المقررة في المؤسسة والتي تهدد معلوماتها وأصولها الأخرى. عند صياغة سياسة أمن المعلومات للحوسبة السحابية، يجب أن يأخذ عميل خدمة السحابة ما يلي في الاعتبار:

- يجوز لمقدم خدمة السحابة الوصول إلى المعلومات المخزّنة في بيئة الحوسبة السحابية وإدارتها؛
- يمكن الاحتفاظ بالأصول في بيئة الحوسبة السحابية، مثل برامج التطبيقات؛
- يمكن تشغيل العمليات على خدمة سحابة ظاهرية متعددة المستأجرين؛
- مستخدمو خدمة السحابة والسياق الذي يستخدمون فيه خدمة السحابة؛
- مسؤولو خدمة السحابة الذين لديهم حق وصول متميز إلى عميل خدمة السحابة؛
- المواقع الجغرافية لمؤسسة مقدم خدمة السحابة والبلدان التي يمكن فيها لمقدم خدمة السحابة تخزين بيانات عميل خدمة السحابة (بما في ذلك التخزين المؤقت).

يجب أن تعرّف سياسة أمان عميل خدمة السحابة ذات الصلة مزود خدمة السحابة بوصفه نوعًا من الموردين، ويجب أن تديره بما يتوافق مع سياسة الأمان. يهدف ذلك إلى الحد من المخاطر التي تنجم عن الوصول إلى بيانات عميل خدمة السحابة المرتبطة بمقدم خدمة السحابة وإدارتها.

يجب أن ينظر عميل خدمة السحابة في القوانين واللوائح التنظيمية ذات الصلة السارية في الاختصاصات القضائية التي تحكم مقدم خدمة السحابة، بالإضافة إلى تلك التي تحكم عميل خدمة السحابة. يجب أن يحصل عميل خدمة السحابة على دليل على امتثال مقدم خدمة السحابة للوائح والمعايير ذات الصلة المطلوبة لإنجاز أعمال عميل خدمة السحابة. ويمكن أن تكون هذه الأدلة أيضًا مصادقات/شهادات صادرة عن مدققين خارجيين.

**يجب على المورِّد إخطار بنك باركليز كتابيًا، بمجرد إمكانية القيام بذلك قانونيًا، بشأن ما إذا كان معرّضًا للاندماج أو الاستحواذ أو أي تغيير آخر في الملكية.**

## MC 2.0 - إدارة المخاطر

يتعين على المورد استحداث برنامج لإدارة الأخطار يعمل على تقييم الأخطار والحد من آثارها ومراقبتها بشكل فعال عبر البيئة التي يتحكم فيها المورّد.

يجب أن يتضمن برنامج إدارة الأخطار، على سبيل المثال لا الحصر، المجالات الآتية:

- يجب أن يضع المُورِّد إطار عمل لإدارة المخاطر (على سبيل المثال، مخاطر المعلومات والمخاطر الإلكترونية والمادية والتقنية، ومخاطر البيانات، والتخطيط لاسترداد البيانات بعد الكوارث). ويجب أن توافق السلطة المنظِّمة المناسبة على الإطار (على سبيل المثال، مجلس الإدارة أو إحدى لجانه). ويجب تضمينه في إستراتيجية الأعمال الشاملة وإطار عمل إدارة المخاطر.
- بالاتساق مع إطار عمل الأخطار، يجب إجراء تقييمات رسمية للأخطار سنويًا على الأقل أو على فترات زمنية محددة، أو يتم إجراؤها بحسب الحدث، كأن تكون استجابة لحادث ما أو للدروس المستفادة منه (وبالاقتران مع أي تغييرات في أنظمة المعلومات أو البناء المادي أو المساحة) لتحديد مدى احتمال كل المخاطر المحددة ومدى تأثيرها باستخدام الأساليب الكمية والنوعية. يجب تحديد احتمالية الأخطار المتأصلة والمتبقية وتأثيرها بصورة مستقلة، مع مراعاة كل فئات الأخطار (على سبيل المثال، نتائج التدقيق، وتحليل التهديدات ونقاط الضعف، والامتثال التنظيمي).
- وضع معايير المخاطر والالتزام بها، وهي تتضمن:
  - معايير قبول المخاطر،
  - ومعايير إجراء تقييمات المخاطر،

- تحديد المخاطر:
  - تطبيق إجراءات تقييم المخاطر لتحديد مخاطر فقدان سرية المعلومات وسلامتها وتوافرها ضمن نطاق إطار عمل المخاطر،
  - وتحديد الأشخاص المسؤولين عند التعامل مع المخاطر،
- تحليل المخاطر:
  - تقييم العواقب المحتملة التي قد تنتج إذا تم تحديد المخاطر،
  - وتقييم الاحتمالية الواقعية لحدوث المخاطر المحددة،
  - وتحديد مستويات الخطورة
- تقييم المخاطر:
  - المقارنة بين نتائج تحليل المخاطر ومعايير المخاطر المقررة،
  - وإعطاء الأولوية للمخاطر التي تم تحليلها عند معالجة المخاطر
- معالجة المخاطر:
  - تحديد خيارات معالجة المخاطر المناسبة، مع مراعاة نتائج تقييم المخاطر،
  - وتحديد كل الضوابط اللازمة لتنفيذ خيار (خيارات) علاج المخاطر المختارة،
  - وإصدار بيان قابلية تطبيق يتضمن الضوابط الضرورية ومبرر عمليات التضمين، سواء تم تنفيذها أم لا،
  - ويجب على المورد التأكّد من تقليل الأخطار التي تم تحديدها أو القضاء عليها في البيئة من خلال ترتيب أولويات الأخطار وتنفيذ التدابير المضادة. وينبغي للمُورّد مراقبة التدابير المضادة باستمرار لكي تتسم بالفعالية.
- يجب أن يُجري المورّد تقييمًا للمخاطر بصفة سنوية كحد أدنى في ما يتعلق بأمن المعلومات والأمن الإلكتروني والأمن المادي وخصوصية البيانات/حماية البيانات والتخطيط لاسترداد البيانات بعد الكوارث. يجب أن يراعي المُورّد وتيرة أكثر تكرارًا، بناءً على البيئات المحددة التي تشتمل على تهديدات حالية وناشئة.
  - تقييم المواقع المهمة لتشغيل العمليات/الخدمات المقدمة إلى بنك باركليز سنويًا على الأقل (بما في ذلك مراكز البيانات)
- يجب أن تحتفظ المؤسسة بمعلومات موثقة حول عملية تقييم مخاطر أمن المعلومات.
- يجب أن تراعي تقييمات الأخطار المرتبطة بمتطلبات حوكمة البيانات ما يأتي:
  - تصنيف البيانات وحمايتها من الاستخدام والوصول والضياع والإتلاف والتزوير على نحو غير مصرح به.
  - الوعي بمواقع تخزين البيانات الحساسة ونقلها عبر التطبيقات وقواعد البيانات والخوادم والبنية التحتية للشبكة.
  - الامتثال لفترات الاحتفاظ المحددة ومتطلبات التخلص في نهاية فترة البيانات.
- يجب أن يجري المورّد تقييم تأثيرات الخصوصية وكيف يمكن أن تؤدي مخاطر الخصوصية من هذا القبيل إلى تأثيرات متابعة على العمليات التنظيمية، بما في ذلك أولويات المهمة والأقسام وأولويات إدارة المخاطر الأخرى (مثل الامتثال والشؤون المالية) والسمعة والقوة العاملة، والثقافة.
- يجب على المورد أن يطور هيكل حوكمة مؤسسيًّا وأن ينفذه لتمكين الفهم المستمر لأولويات إدارة المخاطر داخل المؤسسة التي تبرزها مخاطر الخصوصية

**يجب على المورد إخطار بنك باركليز عما إذا كان غير قادر على معالجة أي جوانب للأخطار أو تخفيف حدتها بشكل جوهري، وهو ما قد يؤثر في الخدمة المقدمة إلى بنك باركليز. يجب إبلاغ بنك باركليز بهذه الحالات على الفور لتمكينه من الامتثال لأي التزامات إبلاغ تنظيمية، وخلال 10 أيام عمل من الاكتشاف على أي حال.**

## MC 3.0 - الأدوار والمسؤوليات

يعدُّ المورّد مسؤولاً عن ضمان أن جميع موظفيه، بما في ذلك، على سبيل المثال لا الحصر، المتعهدون والمتعهدون من الباطن ومعالجو البيانات من الباطن المشاركون في تقديم الخدمة إلى بنك باركليز، على دراية بمتطلبات الرقابة في بنك باركليز ويلتزمون بها. يجب أن يضمن المورّد تعيين فريق مناسب من الاختصاصيين و/أو الأفراد الذين يتمتعون بمهارات متناسبة ومتساوية وأدوار ومسؤوليات محددة لدعم و/أو إدارة المتطلبات الرقابية المتبعة في بنك باركليز للعمل بشكل فعّال من أجل حماية الخدمة (الخدمات) المقدمة إلى بنك باركليز.

يجب على المورّد تحديد الأدوار والمسؤوليات وإبلاغها للموظفين لتقديم الدعم الفعال للمتطلبات الرقابية في بنك باركليز. تجب مراجعة الأدوار والمسؤوليات بشكل منتظم (وفي كل الأحوال، لا تقل الوتيرة عن مرة واحدة كل 12 شهرًا) وبعد إجراء أي تغيير جوهري في النموذج التشغيلي للمورّد أو أعماله.

يتحمل المورّد مسؤولية التأكّد من أن الموظفين والمتعهدين والمتعهدين من الباطن/معالجي البيانات من الباطن على دراية بالمتطلبات الرقابية الواردة في هذا المعيار والسياسات والمعايير ذات الصلة به. يجب على المُورّد تعيين جهة اتصال للتواصل مع بنك باركليز بشأن أي تصعيد ينشأ عن عدم الامتثال للمتطلبات الرقابية. يجب تيسير نقل المتطلبات التعاقدية المحددة كتابةً إلى المتعهدين/معالجي البيانات من الباطن التابعين للمورّد.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب أن يتفق عميل خدمة السحابة مع مقدم خدمة السحابة على تخصيص مناسب للأدوار والمسؤوليات المتعلقة بأمن المعلومات، وأن يؤكد على أنه يمكنه الوفاء بالأدوار والمسؤوليات المخصصة له. وينبغي أن ينص اتفاق ما على أدوار ومسؤوليات كلا الطرفين. يجب أن يحدد عميل خدمة السحابة علاقته بقسم دعم العملاء والعناية بهم لدى مقدم خدمة السحابة وعليه أن يتولى إدارتها.

يجب أن يحدد عميل خدمة السحابة سياساته وإجراءاته الحالية أو يمدد العمل بها بما يتوافق مع استخدامه لخدمات السحابة، وأن يُطلع مستخدمي خدمة السحابة على أدوارهم ومسؤولياتهم في أثناء استخدام خدمة السحابة.

## MC 4.0 - التعليم والتوعية

يجب أن يقوم المورّد بإدارة برنامج تدريبي توعوي مستمر لجميع الموظفين التابعين للمورّد بما في ذلك المتعهدون، والموظفون المعيّنون لفترات قصيرة، والاستشاريون. ويجب أن يتلقى جميع الأفراد الذين لديهم إمكانية الوصول إلى بيانات/معلومات بنك باركليز أو أصوله المادية الأخرى تدريبًا مناسبًا وتحديثات توعوية منتظمة في ما يتعلق بالسياسات والعمليات والإجراءات التنظيمية المتعلقة بوظيفتهم المهنية ضمن نطاق المؤسسة. يجب أن تؤدي مستويات التدريب والتوعية إلى تجهيز الموظفين العاملين لدى المورّد لأداء أدوارهم بشكل آمن. يجب تسجيل سجلات البرنامج الجاري تنفيذه في منصة إدارة تعلم مناسبة أو من خلال عملية يدوية.

يجب على المورّد التأكّد من أن جميع الموظفين العاملين لدى المورّد قد أكملوا البرنامج التدريبي الإلزامي المتعلق بتثقيف الموظفين وتوعيتهم، ويشمل ذلك الأمن الإلكتروني والأمن المادي والتخطيط لاسترداد البيانات بعد الكوارث وإدارة المعلومات الشخصية (خصوصية البيانات/حماية البيانات) وإدارة البيانات وإدارة خدمات تكنولوجيا المعلومات وضوابط EUDA وحماية بيانات بنك باركليز في غضون **شهر واحد من انضمامه** إلى المؤسسة و/أو عند انضمامه إلى خدمة (خدمات) بنك باركليز. إلى جانب تحديث التدريب سنويًّا، يجب على المورّد التكفل بإقامة اختبار للتحقق من فهم الموظفين لديه للتدريب والتوعية. يجب تسجيل كل البرامج التدريبية المقدمة والاحتفاظ بها لمنفعة جميع الموظفين العاملين لدى المورّد الذين يقدمون الخدمة (الخدمات) إلى بنك باركليز، ويجب تقديمها إلى بنك باركليز - عند الطلب - لتفحّصها.

يجب على المورّد التأكد من أن برنامجه التدريبي التوعوي يشمل مواضيع الأمن الإلكتروني، مثل الهندسة الاجتماعية وتهديدات المصادر المطلعة، ويوصى بأن يجري المورّد اختبارات محاكاة على هجمات الهندسة الاجتماعية باستخدام تقنيات، مثل اختبارات عمليات محاكاة التصيّد الاحتيالي، لجميع الموظفين على مستوى المؤسسة مع ضرورة المراقبة المستمرة للتأكد من فهم فداحة هذه المخاطر بوضوح والتخفيف من حدة المشاكل المحددة.

يجب أن تتلقى المجموعات المعرّضة لمستويات عالية من الخطورة، مثل هؤلاء الذين يمكنهم الوصول إلى النظام (الأنظمة) المميز أو إلى المساحات العالية الخطورة أو الحرجة أو العاملين في أقسام حساسة (بما في ذلك المستخدمون المتميزون، ومنهم المطورون، وقسم الدعم، وكبار المسؤولين التنفيذيين وموظفو أمن المعلومات والجهات المعنية الخارجية)، تدريبًا توعويًّا مؤسسيًّا بخصوص أمن المعلومات والأمن المادي حسب الأدوار والمسؤوليات المنوطة بهم.

يجب أن يتم إشراك جميع موظفي الأمن المادي (سواء أكانوا موظفين لدى المورّد أم مالكي عقار أم مورّدين خارجيين) أو التعاقد معهم من خلال مقدم خدمة معتمد ومرخّص له وفقًا للتشريعات المحلية، وأن يتم منحهم ترخيصًا شخصيًا، عند الاقتضاء حسب الاختصاص القضائي، للقيام بمهام أمنية. ويجب أن يتلقى أفراد الأمن المادي تدريبًا أمنيًّا يتناسب مع الأدوار والمسؤوليات المنوطة بهم. يجب توثيق كل البرامج التدريبية المقدمة ويجب الاحتفاظ بسجل التدريب لمنفعة جميع موظفي الأمن، ويجب تقديمها إلى بنك باركليز - عند الطلب - لتفحّصها

يجب على المورّد أن يكفل تدريب موظفيه الخارجيين المشاركين في معالجة البيانات على التثقيف التوعوي بشأن الخصوصية لأداء واجباتهم ومسؤولياتهم المتعلقة بالخصوصية بشكل فعّال بما يتوافق مع السياسات والعمليات والإجراءات والاتفاقيات وقيم الخصوصية المؤسسية ذات الصلة. يجب توثيق كل البرامج التدريبية المقدمة ويجب الاحتفاظ بسجل التدريب لمنفعة جميع الموظفين، ويجب تقديمها إلى بنك باركليز - عند الطلب - لتفحّصها

يجب على المورّد تدريب الموظفين على أداء واجباتهم في إدارة البيانات (إدارة عناصر البيانات المهمة أو التطبيقات المُدارة بواسطة جهة خارجية) بفعالية.

يجب على جهة اتصال ضوابط EUDA لدى المورّد تحديد الموظفين العاملين لدى المورّد الذين تُناط بهم مسؤوليات ضوابط EUDA وضمان إتمامهم التدريب الخاص بالتثقيف والتوعية المناسب لدورهم الوظيفي مرةً واحدةً على الأقل كلَّ عام والاحتفاظ بدليل يثبت الامتثال للضوابط.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب أن يضيف عميل خدمة السحابة العناصر التالية إلى برامج التوعية والتثقيف والتدريب لمنفعة مديري أعمال خدمة السحابة ومسؤولي خدمة السحابة وموظفي دمج خدمة السحابة ومستخدمي خدمة السحابة، بما في ذلك الموظفون والمتعهدون المعيّنون:

- معايير استخدام خدمات السحابة وإجراءاتها؛
- مخاطر أمن المعلومات المرتبطة بخدمات السحابة وكيفية إدارة هذه المخاطر؛
- مخاطر بيئة النظام والشبكة عند استخدام خدمات السحابة؛
- الاعتبارات القانونية والتنظيمية المعمول بها.

يجب توفير برامج التوعية والتثقيف والتدريب بخصوص أمن المعلومات والتي تتمحور حول خدمات السحابة للإدارة وللمديرين المشرفين، بما في ذلك وحدات الأعمال. تدعم هذه الجهود التنسيق الفعّال لأنشطة أمن المعلومات.

## MC 5.0 - إدارة الحوادث

يجب أن يضع المورّد إطار عمل راسخًا لإدارة الحوادث بهدف إدارة حادث وسببه الأساسي الناجم من بيئة المورّد وكذلك احتوائه والقضاء على حدّة آثاره أو التخفيف منها.

يجب على المورّد تبني إجراء إدارة حوادث وأزمات يتضمن عملية خاصة بتصعيد الحوادث/الأزمات إلى بنك باركليز. يجب على المورّد التكفل بإخضاع فرق الاستجابة للحوادث/الأزمات وعملياتها للاختبار، وذلك بمعدل مرة واحدة سنويًا على الأقل، لإثبات قدرته على الاستجابة لأي حوادث بفعالية وكفاءة. يجب أن يختبر المُورّد أيضًا قدرته على إبلاغ جهات الاتصال المعنية بالحادث ضمن جدول زمني محدد وإثبات ذلك لبنك باركليز عندما يُطلب منه ذلك.

ويجب على المورد وضع خطط استجابة جيدة التوثيق للحوادث بحيث تحدد أدوار الموظفين التابعين للمورّد وكذلك مراحل التعامل مع/إدارة الحوادث:

- المسؤوليات والإجراءات - يجب تحديد مسؤوليات الإدارة وإجراءاتها لضمان الاستجابة السريعة والفعالة والمنظمة للحوادث.
- الإبلاغ عن وقائع الحوادث – يجب الإبلاغ عن وقائع الحوادث عبر قنوات الإدارة المناسبة في أسرع وقت ممكن ويجب أن تكون آلية الإبلاغ سهلة ومتاحة لجميع الموظفين العاملين لدى المورّد والمتعهدين التابعين له.
- تقييم وقائع الحوادث - يجب تقييم وقائع الحوادث لتحديد درجة الخطورة والتصنيف المناسبين والاستجابة المطلوبة.
  - تصنيف الحوادث - عليك وضع مقياس لتصنيف الحوادث وتحديد ما إذا كان يجب تصنيف الواقعة بأنها حادث أم لا. يمكن أن يساعد تصنيف الحوادث وتحديد أولوياتها في تحديد تأثير الحادث ومداه.
- الاستجابة للحوادث - تجب الاستجابة للحوادث وفقًا للإجراءات الموثقة لدى قسم إدارة الحوادث التابع للمورّد.
  - احتواء الحادثة - عليك الاستفادة من القدرات البشرية والعمليات والتكنولوجيا لاحتواء أي حادثة تشهدها البيئة بسرعة وفعالية.
  - إزالة/تخفيف حدّة التهديد - الاستفادة من القدرات البشرية والعمليات والتكنولوجيا لإزالة/تخفيف حدّة التهديد الأمني و/أو مكوناته الناجمة من البيئة بسرعة وفعالية.
- الاستفادة من الحوادث - يجب استخدام المعرفة المكتسبة من تحليل الحوادث وحلها للحدّ من احتمالية وقوع الحوادث في المستقبل أو من تأثيرها.
- جمع الأدلة - يحدد المورّد إجراءات تحديد المعلومات وجمعها وحيازتها وحفظها، ويقوم بتطبيق هذه الإجراءات؛ فهذه يمكن أن تكون بمثابة دليل.

بعد الحادثة - بعد انقطاع خدمة (خدمات) مقدمة إلى بنك باركليز، يجب تقديم **تقرير ما بعد الحادث** إلى بنك باركليز في غضون **أربعة أسابيع تقويمية** من استعادة الخدمة إلى مستويات التشغيل العادية. يلزم أن يتضمن التقرير مراجعة لما يأتي كحد أدنى:

- الأحداث المحيطة بالوضع؛
- كيفية إدارة الحادث/الأزمة؛
- تحليل سبب الحدوث الجذري لها؛
- ما إذا كان قد تم تصنيفه بوصفه "حدثًا خطرًا" من جانب المورّد أو بنك باركليز أم لا (أي يُعد مهمًا بدرجة توجب الإبلاغ عنه/تصعيده إلى المساهمين المعنيين وفق السياسات المعمول بها والمعروفة لدى المورد)؛
- وما إذا كان يمثل "مخاطر سلوكية" أم لا (كأن يكون المورد يتعامل مباشرةً مع عملاء بنك باركليز)؛
- وأيَّ تعويض مستحق لعملاء بنك باركليز معروف للمورد،
- والتحسين المستمر لمنع التكرار،
- ويجب أن يسعى المورّد إلى إثبات تحسين أنشطة الاستجابة حيثما أمكن من خلال دمج الدروس المستفادة من أنشطة الاكتشاف/الاستجابة الحالية والسابقة.

بالنسبة إلى الاتصال - يجب على المورّد تعيين نقطة اتصال تتواصل مع بنك باركليز في حال وقوع حادثة/أزمة ما. يجب على المورِّد إخطار بنك باركليز بتفاصيل الاتصال بالفرد (الأفراد) وأي تغييرات تطرأ عليها، بما في ذلك أي اتصالات خارج ساعات العمل وأرقام الهواتف.

**يجب أن تتضمن التفاصيل ما يأتي: -الاسم والمسؤوليات داخل المؤسسة والدور وعنوان البريد الإلكتروني ورقم الهاتف**

إذا أكّد المُورّد في أي وقت أن أي حادث يؤثر في الخدمات المقدمة إلى بنك باركليز أو أنظمته أو بياناته، فعلى المُورّد إبلاغ بنك باركليز على الفور وبما لا يتجاوز بأي حال مدة **ساعتين**.

عند علم المورّد بوقوع **حادثة إلكترونية**، بما في ذلك عبر إشعار من كيان تابع لبنك باركليز، يجب على المورّد، فورًا، ولكن بما لا يتجاوز بحال الوقت المطلوب بموجب أحكام القانون المعمول به، أو في غضون **48 ساعة** من العلم لأول مرة بوقوع حادثة أمن إلكتروني إذا لم يوجد مثل هذا الاشتراط، أن يسارع إلى إخطار بنك باركليز عن طريق إرسال بريد إلكتروني إلى العنوان gcsojoc@barclays.com وتقديم كل المعلومات ذات الصلة، بما في ذلك، إن أمكن، (أ) فئات سجلات بيانات بنك باركليز المتضررة وعددها التقريبي، وإن أمكن، فئات مالكي البيانات المتضررين وعددهم التقريبي، و(ب) تأثير حادثة الأمن الإلكتروني في بنك باركليز والعواقب المحتملة لذلك، والأشخاص مالكي البيانات المتضررين إن أمكن، و(ج) الإجراءات التصحيحية والمخففة لحدة الحادثة التي تم اتخاذها أو سيتم اتخاذها من طرف المورّد.

في حال حدوث أي سرقة فعلية أو مشتبه بها أو مزعومة، أو أي استخدام - أو إفشاء غير مصرح به - لأي **بيانات شخصية محمية** بسبب فشل التدابير الوقائية الأمنية للمُورِّد (أو أيّ من موظفي المورّد) أو الوصول غير المصرح به إلى البيانات الشخصية المحمية من المُورّد أو من خلاله (أو أي من موظفي المورّد)، أو فقدان البيانات الشخصية المحمية أو تلفها أو إتلافها مما لدى المُورّد أو في حيازة أي من موظفيه أو ضمن نطاق تحكمهم، أو أي معالجة غير مصرّح بها لأي بيانات شخصية محمية، يجب على المُورّد إبلاغ بنك باركليز في أقرب وقت ممكن، وبما لا يتجاوز، بأي حال، مدة **24 ساعة** من العلم بالحدث ذي الصلة، وذلك من خلال إرسال بريد إلكتروني إلى العنوان gcsojoc@barclays.com، وتقديم كل أوجه التعاون والمساعدة إلى بنك باركليز في ما يتعلق بهذا الحدث، بما في ذلك توفير كل المعلومات ذات الصلة، مثل البيانات ووقت الحادثة وموقعها ونوعها وتأثيرها، وحالتها، والإجراءات التخفيفية المتخذة.

إذا تم استخدام متعهد/معالج بيانات من الباطن لتقديم الخدمة، حيث سيحتفظ ببيانات/معلومات أو أصول بنك باركليز أو يعالجها، يجب على المُورِّد الحصول على موافقة من بنك باركليز. يجب أن تربط المورّد علاقة تعاقدية مع المتعهدين من الباطن/معالجي البيانات من الباطن، ويجب أن يضمن أن يكون المتعهدون من الباطن/معالجو البيانات من الباطن حاصلين على الاعتماد المتعلق بالإطار المعياري المماثل لأفضل الممارسات في المجال، وأنهم يؤدون بفعالية مهمة حماية بيانات/معلومات بنك باركليز التي يعالجونها و/أو يحتفظون بها. في حال وقوع حادث لمتعهد من الباطن/معالج بيانات من الباطن، يجب التأكّد من اتباع إجراء الإبلاغ عن الحادثة أعلاه.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب أن يتحقق عميل خدمة السحابة من توزيع المسؤوليات المرتبطة بإدارة الحوادث، ويجب أن يتأكّد من أنها تستوفي المتطلبات الخاصة به. يجب أن يطلب عميل خدمة السحابة معلومات من مقدم خدمة السحابة حول الآليات الخاصة بما يلي:

– إبلاغ عميل خدمة السحابة مقدم خدمة السحابة عن حادث/حدث اكتشفه؛
– تلقي عميل خدمة السحابة بلاغات حول حادث/حدث اكتشفه مقدم خدمة السحابة؛
– تتبع عميل خدمة السحابة حالة حدث أمن معلومات تم الإبلاغ عنه.

## MC 6.0 – إدارة أصول تكنولوجيا المعلومات (المكونات المادية والبرامج)

يجب أن يضع المُورّد برنامجًا فعّالاً لإدارة الأصول وعليه تنظيمه طوال دورة عمر الأصول. ويجب أن تحكم إدارة الأصول دورة حياتها بدايةً من الاستحواذ إلى السحب و/أو التخلص الآمن منها، مع توفير الرؤية والأمن لكل فئات الأصول في البيئة.

يجب على المورد الاحتفاظ بقائمة جرد كاملة ودقيقة ومحدّثة للأصول التجارية المهمة الموجودة في كل المنصات و/أو المواقع الجغرافية الموجودة ضمن نطاق الخدمة (الخدمات) المقدمة إلى بنك باركليز، بما في ذلك أي معدات تابعة لبنك باركليز تستضيفها منشآت المورد، أو أي متعهدين/معالجي بيانات من الباطن يوفرهم بنك باركليز، والتأكد من إجراء اختبار واحد على الأقل سنويًا للتحقق من أن قائمة جرد أصول المعلومات محدّثة وكاملة ودقيقة، وإبراز النتائج لبنك باركليز عند طلبها.

يجب أن تتناول عملية إدارة الأصول الجوانب الآتية:

- جرد الأصول - يتم تحديد الأصول المرتبطة بالمعلومات ومنشآت معالجة المعلومات ويتم إعداد جرد لهذه الأصول والاحتفاظ به.
  - يجب على المورّد الاحتفاظ بقائمة جرد دقيقة ومحدّثة لكل أصول المكونات المادية لتكنولوجيا المعلومات مع إمكانية تخزين المعلومات أو معالجتها.
  - يجب أن يكون لدى المورّد جرد دقيق ومحدّث لأصول تكنولوجيا المعلومات الخاصة بمعدات بنك باركليز التي يستضيفها المورّد و/أو أصول تكنولوجيا المعلومات الخاصة ببنك باركليز والتي يتم تقديمها للمُورّد.
  - يجب أن يحتفظ المورّد الذي لديه إعداد من الدرجة 1 والدرجة 2 والدرجة 3 بقوائم جرد محدّثة وكاملة ودقيقة للأصول (بما فيها أجهزة الكمبيوتر المكتبية أو أجهزة الكمبيوتر المحمولة أو معدات الشبكة أو رموز RSA المميزة أو أي أصول مقدمة من بنك باركليز).
  - يجب على المورّد إجراء تسوية لكل أصول بنك باركليز (المكونات المادية والبرامج) مرةً واحدةً سنويًّا، وإبلاغ بنك باركليز (مكتب الأمن الرئيس - فريق ECAM) بنتائجها.
  - ويجب الاحتفاظ بجرد محدّث لكل منتجات البرامج المنشورة والمصرّح بها والمطلوبة لتقديم الخدمة إلى بنك باركليز والامتثال لبنود وشروط التراخيص المعنيّة.
  - يجب أن يفسر جرد أصول عميل خدمة السحابة المعلومات والأصول ذات الصلة المخزنة في بيئة الحوسبة السحابية. يجب أن تشير سجلات الجرد إلى مكان الاحتفاظ بالأصول، مثل تحديد خدمة السحابة.
- ملكية الأصول - يجب أن تكون الأصول التي يتم الاحتفاظ بها في الجرد خاضعة للملكية.
  - تتم حماية أصول المعلومات بناءً على تصنيفها وأهميتها وقيمتها التجارية.
- الاستخدام المقبول للأصول - يتم تحديد قواعد الاستخدام المقبول للمعلومات والأصول المرتبطة بالمعلومات ومنشآت معالجة المعلومات وتوثيقها وتنفيذها.
  - تأكّد من إزالة الأصول غير المصرّح بها من الشبكة.
  - يجب على المورد ضمان تنفيذ إجراءات فعالة وكافية للحد من تأثيرات استخدام التكنولوجيات غير المدعومة ونهاية العمر الافتراضي للأصول والبيانات وسحبها والتخلص الآمن منها للقضاء على الخطر
  - ضع علامة على البرامج والمكونات المادية غير المدعومة بأنها غير مدعومة في نظام الجرد.
- إرجاع الأصول - يجب على جميع الموظفين العاملين لدى المورّد والمتعهدين من الباطن/معالجي البيانات من الباطن (في نطاق الخدمة (الخدمات) المقدمة إلى بنك باركليز) إرجاع كل أصول المورّد التي بحوزتهم عند إنهاء توظيفهم أو عقدهم أو اتفاقيتهم.
  - يجب التحقيق في أصول بنك باركليز "المفقودة أو المسروقة" بشكل صحيح وإبلاغ بنك باركليز بها بما يتوافق مع ضوابط إدارة الحوادث.
  - في حالات "فقدان أو سرقة" أصول المورّد التي تحتوي على معلومات إبلاغ بنك باركليز، يجب إبلاغ بنك باركليز عن ذلك وفقًا لضوابط إدارة الحوادث.

يجب على المورّد إبلاغ بنك باركليز على الفور بالتغييرات المؤكدة في قدرته على الدعم، سواء أكان مباشرًا أم غير مباشر، وذلك في ما يتعلق بأصول تكنولوجيا المعلومات المستخدمة في تقديم الخدمات إلى بنك باركليز، بما في ذلك عندما تنطوي المنتجات على نقاط ضعف أمنية، ويجب أن يضمن ترقية أصول تكنولوجيا المعلومات هذه أو سحبها في الوقت المناسب.

نقل أصول باركليز - يضمن المورّد نقل كل أصول بنك باركليز وبياناته بشكل آمن مع فرض ضوابط متناسبة ومتناسقة مع تصنيف الأصول والبيانات التي يتم نقلها وقيمتها (سواء من منظور الضرر المالي أو الإضرار بالسمعة)، مع إدماج بيئة التهديد التي يتم النقل فيها.

**توجيهات لعميل خدمة السحابة (المورّد)**

ينبغي أن يفسر جرد أصول عميل خدمة السحابة المعلومات والأصول ذات الصلة المخزنة في بيئة الحوسبة السحابية. ينبغي أن تشير سجلات الجرد إلى مكان الاحتفاظ بالأصول، مثل تحديد خدمة السحابة.

يمكن أن يؤدي تثبيت البرامج المرخصة تجاريًا في خدمة سحابية إلى خرق شروط ترخيص البرنامج. يجب أن يطبق عميل خدمة السحابة إجراءً لتحديد متطلبات الترخيص الخاصة بالسحابة قبل السماح بتثبيت أي برنامج مرخص في خدمة السحابة. يجب إيلاء اهتمام خاص للحالات التي تكون فيها خدمة السحابة مرنة وقابلة للتوسيع ويمكن تشغيل البرنامج على أنظمة أو مراكز معالجات أكثر مما تسمح به بنود الترخيص.

## MC 7.0 – التخلص/الإتلاف الآمن من الأصول المادية والبيانات المتبقية من المعلومات الإلكترونية

يجب تنفيذ إتلاف أصول معلومات بنك باركليز التي تكون مخزّنة في شكل مادي و/أو إلكتروني، بما في ذلك الصور المستخدمة للخدمة، أو مسحها بطريقة آمنة ومناسبة، ويجب التحقق من أن بيانات بنك باركليز لا يمكن استردادها.

يجب على المورّد تطبيق إجراءات تشتمل على عمليات تجارية وتدابير تقنية داعمة للتخلص من البيانات بشكل آمن باستخدام أساليب التخلّص المناسبة من البيانات، بما في ذلك على سبيل المثال لا الحصر، مسح البيانات التي تعود إلى بنك باركليز وتطهيرها وإتلافها بهدف إزالتها/محوها واستردادها بشكل آمن من كل وسائط التخزين، ما يجعل استرداد بيانات بنك باركليز مستحيلاً بواسطة وسائل الطب الشرعي الحاسوبي المعروفة.

يجب مسح بيانات بنك باركليز المخزَّنة في الوسائط لجعل استرداد البيانات غير ممكن باستخدام أساليب محو البيانات المناسبة، مثل: المسح الآمن أو الإزالة أو محو البيانات أو إتلاف الأصول أو بطريقة مستندة إلى البرامج للكتابة فوق البيانات أو استخدام إطار العمل القياسي للصناعة الخاص بالتخلص من البيانات (NIST). يجب التخلص من كل المعدات (أصول المعلومات) في نهاية عمرها الافتراضي و/أو عمرها التشغيلي (إذا كانت معيبة، أو تم إلغاء خدمتها بسبب توقف الخدمة أو عدم الحاجة إليها، أو استخدامها في تجربة أو إثباتًا لمفهوم، ويمكن استخدام خدمات مسح البيانات للمعدات التي سيُعاد استخدامها، وما إلى ذلك).

تنطبق متطلبات التخلص على المتعهدين من الباطن/معالجي البيانات من الباطن التابعين للمورّد الذين يُستخدمون لتقديم الخدمة إلى بنك باركليز.

يجب التخلص من النسخ الورقية من المعلومات من خلال تمزيقها وفقًا لمعيار P4 DIN66399 على الأقل، وذلك باستخدام أداة سحق الورق (يتضمن هذا معلومات بطاقة الدفع)، أو يمكن حرقها امتثالاً لمعيار BS EN15713:2009.

بالنسبة إلى بنك باركليز، يتعين الاحتفاظ بدليل التخلص من البيانات، مع توفير مسار للمراجعة وأدلة عليه ووسائل لتتبعه، وينبغي أن يتضمن ذلك ما يلي:

- إثبات الإتلاف و/أو التخلص (بما في ذلك تاريخ التنفيذ والطريقة المستخدمة).
- سجلات تدقيق النظام المطلوب حذفها.
- شهادات التخلص من البيانات.
- الأفراد الذين تولوا مهمة التخلص (بما في ذلك، أي شركاء أو أطراف ثالثة أو متعاقدين شاركوا في عملية التخلص).
- يجب إنشاء تقرير إتلاف وتحقق لتأكيد نجاح أي عملية إتلاف/حذف أو فشلها. (أي إن أيَّ عملية كتابة فوق البيانات لا بد أن يتم تقديم تقرير بشأنها يذكر بالتفصيل أي قطاعات تعذر محوها).

في أثناء مغادرة تقديم الخدمة إلى بنك باركليز، يجب على المورّد التأكُّد من إتلاف بيانات بنك باركليز بشكل آمن بناءً على إخطار وتفويض من بنك باركليز.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب أن يطلب عميل خدمة السحابة تأكيدًا بأن مقدم خدمة السحابة يطبق السياسات والإجراءات اللازمة للتخلص الآمن من الموارد أو إعادة استخدامها. ينبغي أن يطلب عميل خدمة السحابة وصفًا موثّقًا لإنهاء عملية الخدمة التي تغطي إرجاع أصول عميل خدمة السحابة وإزالتها، ويتبع ذلك حذف كل نسخ هذه الأصول من أنظمة مقدم خدمة السحابة. يجب أن يسرد الوصف كل الأصول وأن يوثّق الجدول الزمني لإنهاء الخدمة الذي يجب أن يتم في الوقت المناسب.

## MC 8.0 – تصنيف المعلومات ومعالجة البيانات

يجب أن يكون لدى المورد إطار عمل/مخطط مستقر ومناسب لتصنيف المعلومات ومعالجتها (بما يتوافق مع الممارسات الجيدة المعمول بها في الصناعة و/أو متطلبات بنك باركليز) ويجب أن يغطي المكونات الآتية:

- تصنيف المعلومات - يجب تصنيف المعلومات من حيث الأهمية والحساسية للكشف أو التعديل غير المصرح بهما.
- تسمية المعلومات - يجب وضع وتنفيذ مجموعة مناسبة من الإجراءات لتسمية المعلومات وفقًا لمخطط تصنيف المعلومات الذي يتبنّاه المورّد.
- معالجة الأصول - يجب وضع وتنفيذ إجراءات معالجة الأصول وفقًا لمخطط تصنيف المعلومات الذي يتبناه المُورّد.
- ضمان أن يكون جميع الموظفين على دراية بمتطلبات التسمية والمعالجة المعمول بهما لدى المورّد/بنك باركليز وبكيفية تطبيق تصنيف المعلومات الصحيح بطريقة سليمة.

يجب على المورّد الرجوع إلى مخطط تسمية المعلومات ومتطلبات المعالجة من بنك باركليز (**الملحق أ، الجدول أ1 وأ2**)، أو مخطط بديل لضمان قيام المورّد بحماية معلومات بنك باركليز المحفوظة و/أو المعالجة وتأمينها. ينطبق هذا المطلب على كل أصول معلومات بنك باركليز المحفوظة أو المعَالجة نيابةً عن بنك باركليز، بما في ذلك بواسطة المتعهدين/معالجي البيانات من الباطن.

**توجيهات لعميل خدمة السحابة (المورّد)**

يجب أن يقوم عميل خدمة السحابة بتسمية المعلومات والأصول المرتبطة بها التي يتم الاحتفاظ بها في بيئة الحوسبة السحابية وفقًا لإجراءات التسمية التي يعتمدها عميل خدمة السحابة. متى أمكن، يمكن اعتماد الوظائف التي يوفرها مقدم خدمة السحابة والتي تدعم التسمية.

## حق الفحص

يتعين على المورد السماح لبنك باركليز، بناءً على إخطار كتابي من بنك باركليز قبل ما لا يقل عن **عشرة (10) أيام عمل**، بإجراء مراجعة أمنية لأي موقع أو تكنولوجيا يستخدمهما المورد أو المتعهدون/معالجو البيانات من الباطن التابعون له لاستحداث أنظمة المورد المستخدمة في الخدمات أو اختبارها أو تعزيزها أو صيانتها أو تشغيلها، من أجل مراجعة امتثال المورد لالتزاماته تجاه بنك باركليز. يجب على المورّد كذلك السماح لبنك باركليز بإجراء الفحص كل عام على الأقل و/أو فور وقوع حادث أمني.

يجب على بنك باركليز إجراء تقييم مخاطر في ما يتعلق بأي عدم توافق مع الضوابط التي يحددها بنك باركليز في أثناء التفتيش، ويجب على بنك باركليز أن يحدد إطارًا زمنيًا للتصحيح. يجب على المورّد بعد ذلك إكمال أي إصلاح مطلوب خلال هذا الإطار الزمني.

يجب على المورّد تقديم كل المساعدة التي يطلبها بنك باركليز بصورة معقولة في ما يتعلق بأي تفتيش، ويجب تقديم التوثيق في أثناء التفتيش. يجب إكمال الوثائق وإعادتها إلى بنك باركليز على الفور. يجب كذلك على المورّد دعم بنك باركليز بتقديم موجّه أسئلة تقييم مع الدليل المطلوب في أثناء أي مراجعة توكيدية.

## الملحق A: مخطط تسمية المعلومات ومتطلبات معالجة البيانات في بنك باركليز

**الجدول أ1: مخطط التسميات المعلوماتية لبنك باركليز**

| التسمية | التعريف | الأمثلة |
|---|---|---|
| **سرية** | يلزم تصنيف المعلومات بوصفها **سرية** إذا ترتب على الإفصاح غير المصرح به عنها تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار عمل إدارة أخطار المؤسسة (ERMF) بوصفه "مهمًا" (ماليًا أو غير مالي).<br><br>تقتصر هذه المعلومات على جمهور محدد ويجب عدم توزيعها مرة أخرى دون إذن المنشئ. قد يشمل الجمهور المستلمين الخارجيين بتصريح واضح من مالك المعلومات. | • معلومات حول عمليات الدمج أو الاستحواذ المحتملة<br>• معلومات التخطيط الإستراتيجي - التجارية والتنظيمية<br>• معلومات محددة حول تهيئة نظام المعلومات<br>• نتائج تدقيق وتقارير محددة<br>• محاضر اللجنة التنفيذية<br>• تفاصيل المصادقة أو التعريف والتحقُّق (ID&V) - الزبون/العميل والزميل<br>• كميات كبيرة من معلومات حامل البطاقة<br>• توقعات الأرباح أو النتائج المالية السنوية (قبل نشرها للجمهور)<br>• أي بنود مشمولة باتفاقية عدم إفشاء رسمية (NDA) |
| **مقيَّدة - داخلية** | يجب تصنيف المعلومات بوصفها **مقيَّدة - داخلية** إذا كان المستلمون المتوقعون هم فقط الموظفين المعتمدين من بنك باركليز وموفِّري الخدمات المُدارة (MSP) لبنك باركليز بموجب عقد سارٍ قيد التنفيذ، وكانت تقتصر على جمهور معين.<br><br>وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي).<br><br>ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة. | • الإستراتيجيات والميزانيات<br>• تقييم الأداء<br>• رواتب الموظفين وبياناتهم الشخصية<br>• تقييم مدى التأثر |
| **مقيَّدة - خارجية** | يلزم تصنيف المعلومات بوصفها **مقيَّدة - خارجية** إذا كان المستلمون المتوقعون هم فقط الموظفون المعتمدون من بنك باركليز وموفرو الخدمات المُدارة لبنك باركليز بموجب عقد سارٍ قيد التنفيذ، وكانت تقتصر على جمهور معين أو أطراف خارجية مصرح لها من قِبل مالك المعلومات.<br><br>وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي).<br><br>ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة. | • خطط منتجات جديدة<br>• عقود العملاء<br>• العقود القانونية<br>• معلومات الأفراد/معلومات زبائن/عملاء الأحجام المنخفضة المقرر إرسالها خارجيًا<br>• معلومات الزبائن/العملاء.<br>• مواد عرض الإصدار الجديد (مثل نشرة الإصدار، مذكرة العرض)<br>• مستندات البحث النهائية<br>• المعلومات الجوهرية غير العامة وغير التابعة لبنك باركليز (MNPI)<br>• كل التقارير البحثية<br>• المواد التسويقية المحددة<br>• تعليقات السوق<br>• نتائج التدقيق والتقارير |
| **غير مقيدة** | يلزم تصنيف المعلومات بوصفها غير مقيدة إذا كانت معدة للتوزيع العام، أو لن يكون لها أي تأثير سلبي في المؤسسة حال توزيعها. | • المواد التسويقية<br>• المنشورات |

| | | |
|---|---|---|
| | | • الإعلانات العامة<br>• إعلانات الوظائف<br>• المعلومات التي لا تأثير لها في بنك باركليز |

**الجدول أ2: مخطط تسمية المعلومات في بنك باركليز - متطلبات معالجة البيانات**

*** يمكن تصنيف المعلومات ونتائج التدقيق والسجلات الشخصية التي تتعلق بتهيئة أمن النظام بوصفها مقيَّدة – داخلية أو سرية، بناءً على أثر الإفصاح غير المصرح به للأعمال

| مرحلة دورة الحياة | سرية | مقيَّدة – داخلية | مقيَّدة – خارجية |
|---|---|---|---|
| **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) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها.<br>• يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مخولين عليها.<br>• تجب حماية جميع المفاتيح الخاصة المستخدمة لحماية بيانات بنك باركليز و/أو هويتها و/أو سمعتها بموجب المستوى 3 للمعيار FIPS 140-2 أو المعيار الأعلى لوحدات أمن الأجهزة المعتمدة (HSM). | • يلزم عدم تخزين الأصول (سواء أكانت مادية أم إلكترونية) في مواقع عامة (ومن بينها المواقع العامة داخل المنشآت والتي قد يكون للزوار فيها وصول غير خاضع للإشراف).<br>• يلزم عدم ترك المعلومات في الأماكن العامة داخل المنشآت حيث قد يكون للزوار وصول غير خاضع للإشراف. | • لا يتعين تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول أفراد غير مخولين إلى هذه الأصول أو اطلاعهم عليها.<br>• يتعين حماية الأصول الإلكترونية المخزنة عن طريق ضوابط تشفير أو تعويض مناسبة وذلك في حال وجود خطر جسيم يتعلق باحتمالية اطلاع أفراد غير مخولين عليها. |
| **الوصول والاستخدام** | • يلزم عدم العمل على الأصول (سواء أكانت مادية أم إلكترونية) أو تركها من دون مراقبة حيث قد يتمكن الأشخاص غير المصرح لهم من عرضها أو الوصول إليها. لكن يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل: شاشات الخصوصية).<br>• يتعين طباعة الأصول من خلال استخدام أدوات طباعة آمنة.<br>• يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة | • يلزم عدم ترك الأصول (سواء أكانت ورقية أم إلكترونية) في أماكن عامة تقع خارج المنشآت.<br>• يلزم عدم ترك الأصول (سواء أكانت مادية أم إلكترونية) في مواقع عامة داخل المنشآت والتي قد يكون للزوار فيها وصول غير خاضع للإشراف.<br>• يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسب إذا تطلب الأمر ذلك | • يلزم عدم العمل على الأصول (سواء أكانت مادية أم إلكترونية) أو تركها من دون مراقبة حيث قد يتمكن الأشخاص غير المصرح لهم من عرضها أو الوصول إليها. لكن يمكن العمل عليها في حال اتباع ضوابط مناسبة (مثل: شاشات الخصوصية).<br>• يلزم استرداد الأصول المطبوعة على الفور من الطابعة. وفي حال عدم التمكن من ذلك، يلزم الاستعانة بأدوات الطباعة الآمنة.<br>• تلزم حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة. |
| **المشاركة** | • يتعين إرفاق ملصق معلوماتي واضح على كل صفحة من صفحات الأصول المطبوعة.<br>• يلزم أن تحمل المغلفات التي تحتوي على أصول مطبوعة ملصقًا معلوماتيًا واضحًا على الجانب الأمامي وأن تكون مختومة بختم ضد العبث. كما يتعين وضع هذه الأصول داخل مغلف ثانوي غير موسوم وذلك قبل توزيعه.<br>• يتعين أن تحتوي الأصول الإلكترونية على ملصق معلوماتي واضح. كما يتعين أن تحمل كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات ملصقًا معلوماتيًا واضحًا. | • يتعين إرفاق ملصق معلوماتي واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير.<br>• يتعين أن تحتوي الأصول الإلكترونية على ملصق معلوماتي واضح.<br>• يجب أن تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من المؤسسة. | • يتعين إرفاق ملصق معلوماتي واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير.<br>• يتعين إرفاق ملصق معلوماتي واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة<br>• يتعين أن تحتوي الأصول الإلكترونية على ملصق معلوماتي واضح. كما يتعين أن تحمل كل صفحة من صفحات النسخ الإلكترونية للمستندات متعددة الصفحات ملصقًا معلوماتيًا واضحًا. |

| | | | |
|---|---|---|---|
| | • يجب أن تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من المؤسسة.<br>• 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.<br>• يجب أن يقتصر توزيع الأصول على الأفراد المخولين بشكل خاص من قبل مالك المعلومات لاستلامها.<br>• ينبغي عدم إرسال الأصول بالفاكس.<br>• يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية.<br>• ينبغي الحفاظ على تسلسل العهدة فيما يتعلق بالأصول الإلكترونية. | • 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 تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من المؤسسة.<br>• 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.<br>• يجب أن يقتصر توزيع الأصول على الأفراد ممن لديهم أعمال تتطلب ذلك.<br>• 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.<br>• يتعين تشفير الأصول الإلكترونية من خلال استخدام آلية حماية تشفيرية معتمدة وذلك عند إرسالها إلى خارج الشبكة الداخلية. |
| **الحفظ والإتلاف** | • يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة.<br>• يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد.<br>• يتعين حذف أية وسائط إعلامية، تم تخزين الأصول الإلكترونية السرية عليها، بشكل مناسب وذلك قبل عملية التخلص منها أو خلالها. | • يتعين أن يتم التخلص من الأصول المطبوعة من خلال وسيلة إتلاف آمنة.<br>• 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.<br>• يتعين حذف نسخ الأصول الإلكترونية من نظام "سلات المحذوفات" أو أي نظام مشابه وذلك في الوقت المحدد. |

## الملحق B: التعريفات

**معلومات بنك باركليز السرية** تعني أي معلومات يتم الحصول عليها بواسطة مدير لدى المورّد أو المورّد نفسه أو أي موظف لدى المورّد (أو أي جهة منهم تمتلك إمكانية الوصول إليها) في ما يتعلق بهذه البنود العامة و/أو أي عقد يرتبط بأي (i) أنشطة تجارية و/أو منتجات و/أو تطويرات لأيٍّ من كيانات بنك باركليز سابقًا أو حاليًا أو مستقبليًا، و/أو (ii) موظفين و/أو عملاء و/أو أطراف مقابلة و/أو أطراف خارجية/موردين و/أو متعهدين تابعين لأي كيان من كيانات بنك باركليز (بخلاف كيانات المورّد)، بما في ذلك كل الملكيات الفكرية التي يملكها أي كيان تابع لبنك باركليز (بما في ذلك عملاً بأي عقد) أو أي من الموردين/المتعهدين من الجهات الخارجية، والبيانات الشخصية المحمية، وهذه البنود العامة، وكل وحدة وكل عقد، والسجلات التي يتم الاحتفاظ بها بموجب أي عقد، وأي معلومات تتعلق بخطط الكيان أو الشخص المعنيّ، و/أو تسعيره، و/أو منهجياته، و/أو عملياته، و/أو بياناته المالية، و/أو حقوق ملكيته الفكرية و/أو أبحاثه و/أو أنظمته و/أو برامجه و/أو تكنولوجيا المعلومات لديه؛

تعني **بيانات بنك باركليز** كل البيانات والمعلومات والنصوص والرسومات وغيرها من المواد المتمثلة في أي وسيطة من الوسائط، بما في ذلك كل الوسائط الإلكترونية أو الضوئية أو المغناطيسية أو المادية التي (i) يمكن للمُورّد الوصول إليها في ما يتصل بأي عقد، أو (ii) يتم توفيرها للمُورّد بواسطة أيٍّ من كيانات بنك باركليز، أو (iii) ينشئها المورّد أو يجمعها أو يعالجها أو يخزنها أو يرسلها في ما يتعلق بأي عقد، باستثناء المواد المملوكة للمورّد؛

تعني **أنظمة بنك باركليز** أنظمة المعلومات الإلكترونية التي تتألف من واحد أو أكثر من المكونات المادية والمعدات والبرامج والأجهزة الطرفية وشبكات الاتصالات المملوكة و/أو المتحكم فيها و/أو المشغّلة و/أو المستخدمة بواسطة أيٍّ من كيانات بنك باركليز؛

يعني **الحادث الإلكتروني** أي حدث، سواء تم التأكد من حدوثه بالفعل أو يعتقد المورّد أو بنك باركليز لأسباب معقولة أنه قد حدث (استنادًا إلى تهديد ذي مصداقية أو معلومات استخباراتية أو غير ذلك)، وهو ما أدى أو قد يؤدي إلى إلحاق خطر محيق (i) بسرية بيانات بنك باركليز أو سلامتها أو توافرها بالكامل، أو (ii) سرية نظام الموردين أو نظام بنك باركليز وسلامته أو توافره وعمله بشكل طبيعي.

يعني **تقييم تأثير حماية البيانات** تقييم تأثير عمليات المعالجة المتصورة في حماية البيانات الشخصية، على النحو الذي تقتضيه تشريعات حماية البيانات؛

يعني **تشريع حماية البيانات**، إلى أقصى حد ينطبق على أداء أي من التزامات الموردين بموجب أي عقد، ما يلي: (i) توجيه الاتحاد الأوروبي بشأن الخصوصية والاتصالات الإلكترونية EC/58/2002 (على النحو الذي يمكن تعديله أو استبداله من وقت إلى آخر)، و(ii) اللائحة العامة لحماية البيانات الصادرة من الاتحاد الأوروبي 679/2016 (أو GDPR)، وقرارات المفوضية الأوروبية وتوجيهاتها، وكل التشريعات التنفيذية الوطنية، و(iii) اللائحة العامة لحماية البيانات (GDPR) في المملكة المتحدة، و(iv) أحكام قانون غرام-ليكس-بيلي المتعلقة بالمعلومات الشخصية غير المتاحة للاطلاع العام، و(v) قانون نقل التأمين الصحي والمساءلة الصادر في عام 1996، و(vi) كل القوانين واللوائح التنظيمية والتوجيهات التنظيمية الأخرى السارية في ما يخص حماية البيانات وخصوصيتها في (أ) أي منطقة اختصاص قضائي يوجد فيها مقر لكيان تابع لبنك باركليز المعنيّ، ويتم فيها تنفيذ التزامات المورّدين، ويعيش فيها صاحب البيانات المعنيّ، أو تتم فيها معالجة أي بيانات شخصية محمية أو تخزينها أو استخدامها و(ب) أي منطقة اختصاص قضائي ينفذ انطلاقًا منها المورّد أيًا من التزاماته بموجب أي عقد؛

تعني **التزامات رقابة خصوصية البيانات** أي لائحة خصوصية بيانات تشكّل جزءًا من اللائحة رقم 7 (التزامات مراقبة المورّد الخارجي)؛

يجب أن يكون **لصاحب البيانات** الأهمية التي تمنحه إياها قوانين حماية البيانات. عندما لا تقدم تشريعات حماية البيانات تعريفًا لهذا المصطلح، فإنه يعني شخصًا طبيعيًّا محدد الهوية أو شخصًا طبيعيًّا يمكن تحديد هويته، بصورة مباشرة أو غير مباشرة، بشكل خاص عن طريق الرجوع إلى معرّف تحديد الهوية، مثل: الاسم أو رقم تحديد الهوية أو بيانات الموقع أو معرّف عبر الإنترنت أو حسب واحد أو أكثر من العوامل الخاصة بالهوية المادية أو الفسيولوجية أو الوراثية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص الطبيعي؛

تعني **اتفاقية نقل البيانات** أي اتفاقية نقل بيانات مبنية على تلك الشروط التي يقرر بنك باركليز بصورة معقولة أنها تضمن أن تحظى البيانات الشخصية ذات الصلة في المملكة المتحدة و/أو البيانات الشخصية في الاتحاد الأوروبي و/أو البيانات الشخصية خارج الاتحاد الأوروبي/خارج المملكة المتحدة (حسب طبيعة الحالة) بضمانات كافية على النحو المنصوص عليه في تشريعات حماية البيانات عند نقلها؛

تعني **الممارسات الجيدة المعمول بها في الصناعة** في ما يتعلق بأي مهمة وأي ظروف ممارسةَ أعلى درجة من المهارة، والاجتهاد، والتعقل، والتبصر المُتوقّع بصورة معقولة من شخص يتمتع بمهارات وخبرة عالية وينخرط في النوع نفسه من المهام وفي ظل الظروف نفسها أو ظروف مماثلة؛

تحمل **البيانات الشخصية** المعنى الذي تمنحه لها تشريعات حماية البيانات. إذا لم تحدد تشريعات حماية البيانات تعريف هذا المصطلح، فإنه يعني أي معلومات تتعلق بصاحب البيانات أو تعرّف هويته بشكل مباشر أو غير مباشر؛

يعني **خرق البيانات الشخصية** المعنى الذي تمنحه إياه تشريعات حماية البيانات. إذا لم تقدم تشريعات حماية البيانات تعريفًا لهذا المصطلح، فإنه يعني أي خرق أمني يؤدي إلى تلف البيانات الشخصية المنقولة أو المخزنة أو المعالجة بأي طريقة بخلاف ذلك أو فقدانها، أو تغييرها، أو الإفصاح غير المصرح به عنها، أو الوصول إليها بشكل عرضي أو غير قانوني؛

تحمل **المعالجة** المعنى الذي تمنحه لها تشريعات حماية البيانات. إذا لم تقدم تشريعات حماية البيانات تعريفًا لهذا المصطلح، فإنه يعني أي عملية أو مجموعة من العمليات يتم تنفيذها على البيانات الشخصية، سواء أكان ذلك بوسائل أوتوماتيكية أم لا، مثل (على سبيل المثال لا الحصر) جمع البيانات أو تسجيلها أو تنظيمها أو تخزينها أو تعديلها أو تغييرها أو استردادها أو إخضاعها لاستشارات أو استخدامها أو الكشف عنها عن طريق النقل أو النشر أو إتاحتها بأي طريقة أخرى بخلاف ذلك، أو تنسيقها أو توليفها أو حظرها أو محوها أو إتلافها، وسوف يحظى مصطلح **المعالجة** ومصطلح **تمت معالجته** بمعانٍ مشابهة؛

يعني **المتعهد من الباطن** أي جهة خارجية تقوم من وقت لآخر بتوفير السلع و/أو الخدمات في ما يتصل بما يلي: (أ) توفير المنتجات و/أو الخدمات و/أو التسليمات؛ و/أو (ب) معالجة أي بيانات شخصية محمية أو أي استخدام آخر لها وفقًا لما يسمح به العقد؛

يعني **المورّد/موظفو الجهات الخارجية** جميع الأشخاص و/أو الكيانات التي تؤدي أي جزء من الخدمات أو توفر أي منتج (منتجات) بموجب أي عقد، بما في ذلك الموظفون و/أو المتعهدون من الباطن و/أو وكلاء المورّد أو أيّ من متعهديه من الباطن؛

تعني **أنظمة الموردين/الجهات الخارجية** أي أنظمة معلومات إلكترونية (قد تشمل واحدًا أو أكثر من المكونات المادية والمعدات والبرامج والأجهزة الطرفية وشبكات الاتصالات) تكون (هي أو جزء منها): (i) مُستخدمة لتزويد أي شركة تابعة لبنك باركليز بأي منتجات أو خدمات بموجب عقد ما، أو (ii) في حوزة مُورّد أو متعهد من الباطن أو تحت إدارته أو مراقبته أو سيطرته بموجب عقد ما؛

يعني **النظام** أي نظام معلومات إلكتروني (قد يشمل واحدًا أو أكثر من المكونات المادية والمعدات والبرامج والأجهزة الطرفية وشبكات الاتصالات) يُستخدم (أو جزء منه) لتوفير أي سلع أو خدمات إلى أي شركة تابعة لبنك باركليز بموجب عقد ما؛