External Supplier Control Obligation

الأمن المعلوماتي والسيبراني (ICS)

الإصدار 11.0، بتاريخ أكتوبر 2021

مجال/عنوان الرقابة	وصف الرقابة	الأهمية
1. حوكمة أمن المعلومات/الأمن السيبراني، إطار العمل	يجب أن يكون لدى المورّد إطار عمل قياسي بالنسبة للصناعة ثابت ومتسق خاص بحوكمة أمن المعلومات/الأمن السيبراني وفقًا لأفضل ممارسات الصناعة (تتضمن أفضل برامج الصناعة الحالية NIST و ISO/IEC 27001 و ITIL و COBIT) بالإضافة إلى أي متطلبات قابلة للتطبيق في الصناعة. وهذا الأمر سيُمكّن المورّد من التأكُّد من وجود ضمانات أو إجراءات مضادة في عملياته وتقنياته وبيئته المادية. يجب أن يضمن برنامج حوكمة المعلومات المنظَّم جيدًا على مستوى المؤسسة دعم المفاهيم الأساسية للتوافر والسلامة والسريَّة من خلال ضوابط كافية مصممة خصوصًا لتخفيف مخاطر فقدان المعلومات أو تعطُّلها أو تلفها، أو الحد منها؛ كما يجب أن يتأكَّد المورّد من وجود ضوابط لمتطلبات بنك باركليز وأنها تعمل بفاعلية لحماية الخدمة (الخدمات) التي يُقدّمها بنك باركليز. لا بد من وضع إطار عمل لحوكمة الأمن وتوثيقه والموافقة عليه وتنفيذه، وهذا الإطار يشتمل على ضمانات إدارية وتنظيمية وفنية ومادية لحماية الأصول والبيانات من الفقدان وسوء الاستخدام والوصول والكشف والتعديل والإتلاف غير المصرَّح به. يجب أن يشتمل برنامج الأمن -على سبيل المثال لا الحصر- على المجالات الآتية: • برنامج خاص بالسياسة والإجراءات والمعايير يضفي تأثيرًا في سياسة أمن المعلومات والأمن السيبراني بالإضافة إلى تنفيذ المعايير؛ مع تطبيق هذا التأثير بفاعلية وقياسه باستمرار. • برنامج أمن شامل مزوَّد بهيكل واضح للقيادة وآليات تصعيد وإشراف تنفيذي لبث ثقافة المساءلة والوعي بالأمان. • سياسات وإجراءات وعمليات تتم الموافقة عليها وتناقلها عبر المؤسسة. • التأكُّد من خضوع سياسات وإجراءات/معايير أمن المعلومات والأمن السيبراني لمراجعة روتينية (مرة واحدة سنويًا على الأقل أو عند حدوث أي تغييرات مادية) وتكيُّفها بما يتماشى مع ممارسات الأمن السيبراني الحالية وساحة التهديد المتنامي. • ينبغي للمورّد التأكُّد من وجود مساءلة فردية عن المعلومات والأنظمة الأمنية من خلال ضمان وجود ملكية مناسبة لبيئات العمل والمعلومات والأنظمة الأمنية المهمة وتعيينها للأفراد القادرين. • يقوم المورّد بتنسيق الأدوار والمسؤوليات الخاصة بالموظفين ومواءمتها، مع تطبيق سياسة إستراتيجية الأمن وإطار عمله مع الشركاء الداخليين والخارجيين وإدارتها ومراقبة مدى فاعليتها. • ينبغي للمورّد تنفيذ بنية تحتية آمنة وإطار عمل للمراقبة لحماية المؤسسة من أي تهديدات (بما في ذلك الأمن السيبراني) • ينبغي إجراء مراجعات وتقييمات مستقلة بواسطة الخبراء مرة واحدة سنويًا على الأقل لضمان معالجة المؤسسة حالات عدم التطابق بين السياسات والمعايير والإجراءات والتزامات الامتثال المعمول بها. **يجب على المورّد التأكُّد من إخطار بنك باركليز (كتابيًا)، بمجرد إمكانية القيام بذلك قانونيًا، بما إذا كان عرضة للاندماج أو الاستحواذ أو أي تغيير آخر في الملكية.**	إذا لم يتم تنفيذ هذا المبدأ، فقد لا يتمكن بنك باركليز أو مورّدوه أو تكون لديهم القدرة على إثبات الإشراف الملائم على أمن المعلومات/الأمن السيبراني. يحدِّد إطار حوكمة الأمن القوي مستوى أمن المؤسسة بأكملها.

2. إدارة المخاطر الأمنية	يجب على المورّد وضع برنامج لإدارة المخاطر الأمنية يعمل على تقييم المخاطر الأمنية المتنامية وتخفيفها ومراقبتها بفاعلية عبر البيئة التي يتحكم فيها المورّد. يجب أن يتضمن برنامج إدارة الأخطار، على سبيل المثال لا الحصر، المجالات الآتية: • ينبغي أن يكون لدى المورّد إطار عمل لإدارة المخاطر الأمنية معتمد من السلطة الحاكمة المناسبة (مثل: مجلس الإدارة أو إحدى لجانه). وينبغي تضمينه في إستراتيجية الأعمال الشاملة وإطار عمل إدارة المخاطر. • اتساقًا مع إطار عمل المخاطر، ينبغي إجراء تقييمات رسمية للمخاطر مرة واحدة سنويًا على الأقل أو على فترات زمنية محددة، أو يتم إجراؤها حسب الحدث، كأن تكون استجابة لحادث ما أو للدروس المستفادة منه (وبالاقتران مع أي تغييرات في أنظمة المعلومات) لتحديد مدى احتمال كل المخاطر المحددة ومدى تأثيرها باستخدام الأساليب الكمية والنوعية. ينبغي تحديد الاحتمال والتأثير المرتبطين بالأخطار المتأصلة والمتبقية بصورة مستقلة، مع مراعاة جميع فئات الأخطار (على سبيل المثال، نتائج التدقيق، وتحليل التهديدات ونقاط الضعف، والامتثال التنظيمي). • تحديد خيارات معالجة المخاطر الأمنية المناسبة، مع مراعاة نتائج تقييم المخاطر. • صياغة خطة معالجة المخاطر الأمنية، ومعايير قبول المخاطر من خلال أفراد مؤهلين وخاضعين للمساءلة على نحو ملائم. ينبغي أن تتضمن هذه المعايير، على سبيل المثال لا الحصر، حساسية هذه البيانات وأهميتها التجارية. • ينبغي للمورّد التأكُّد من تقليل المخاطر المحدَّدة أو القضاء عليها في البيئة من خلال ترتيب أولويات المخاطر وتنفيذ التدابير الوقائية. • ينبغي تخفيف حدة المخاطر إلى مستوى مقبول. يجب وضع مستويات القبول المستندة إلى معايير الأخطار وتوثيقها وفق الأطر الزمنية المعقولة للحل وموافقة أصحاب المصلحة. • ينبغي أن تراعي تقييمات الأخطار المرتبطة بمتطلبات حوكمة البيانات ما يأتي: ○ تصنيف البيانات وحمايتها من الاستخدام غير المصرَّح به والإفصاح والوصول والفقدان والتدمير والتعديل والتزوير. ○ الوعي بمواقع تخزين البيانات الحساسة ونقلها عبر التطبيقات وقواعد البيانات والخوادم والبنية التحتية للشبكة. ○ الامتثال لفترات الاحتفاظ المحددة ومتطلبات التخلص في نهاية فترة البيانات. • ينبغي للمورّد إجراء تقييم سنوي للمخاطر الأمنية كحد أدنى فيما يتعلق بالأمن واستنادًا إلى البيئات المحدَّدة، مع التفكير في معدل أكثر تواترًا. **إذا كان المورّد غير قادر على معالجة أي جوانب مادية للمخاطر التي قد تؤثر في بيانات بنك باركليز و/أو الخدمة المقدَّمة إلى بنك باركليز، أو الحد منها، فيجب عليه تسجيل ذلك وإخطار بنك باركليز به.**	إذا لم يتم تنفيذ هذه المراقبة، فقد لا يتمكن المورّدون من إظهار الإجراءات المناسبة التي يتم تطبيقها لإدارة المخاطر الأمنية.
3. الأدوار والمسؤوليات	تقع على عاتق المورّد مسؤولية التأكُّد من أنَّ جميع الأفراد المشاركين في تقديم الخدمة إلى بنك باركليز على دراية بمتطلبات المراقبة في بنك باركليز الواردة في هذه الوثيقة، ويلتزمون بها. بالنسبة إلى متطلبات المراقبة في بنك باركليز، ينبغي للمورّدين التأكُّد من وجود فريق متخصص مناسب و/أو أفراد يتمتعون بالمهارات المناسبة، مع أدوار ومسؤوليات محدَّدة لإدارة متطلبات المراقبة في بنك باركليز، وأنها تعمل بفاعلية لحماية الخدمة (الخدمات) التي يُقدِّمها بنك باركليز.	يدعم التحديد الواضح للأدوار والمسؤوليات تنفيذ مركز عمليات الأمان الخاص بأمن المعلومات والأمن السيبراني

	يجب على المورّد تحديد الأدوار والمسؤوليات ومشاركتها فيما يتعلق بجميع مجالات الأمان التي يغطيها مطلب المراقبة. وتلزم مراجعتها بشكل منتظم (وفي جميع الأحوال، لا تقل الوتيرة عن مرة واحدة كل 12 شهرًا) وبعد إجراء أي تغيير جوهري في نموذج تشغيل المورّد أو أعماله. يجب أن تتضمن الأدوار الأساسية مسؤولاً تنفيذيًا كبيرًا يناط به أمن المعلومات والأمن السيبراني. تقع على عاتق المورّد مسؤولية التأكُّد من أنَّ الموظفين/العاملين لديه على دراية بمتطلبات المراقبة المتعلقة بهذا المعيار وما يرتبط بها من سياسات ومعايير، والامتثال لها. يتعين على المورّد تعيين نقطة اتصال خاصة بأي تصعيد للتواصل مع بنك باركليز.	
4. الاستخدام المعتمد	ينبغي للمورّد إعداد متطلبات الاستخدام المقبول ونشرها بهدف إخطار جميع الأفراد العاملين لديه (بما في ذلك المتعاقدون ومستخدمو أنظمة المؤسسة التابعون لأطراف ثالثة) بمسؤولياتهم. تجب مراعاة الموضوعات الآتية: • استخدام الإنترنت، • الاستخدام المستند إلى البرامج كخدمة ((SaaS، • استخدام مستودع الشفرات العام، • استخدام المكونات الإضافية والبرامج المجانية/البرامج التجريبية المستندة إلى المتصفح، • استخدام وسائل التواصل الاجتماعي، • استخدام البريد الإلكتروني للشركة، • استخدام المراسلات الفورية، • استخدام تجهيزات تكنولوجيا المعلومات التي يوفرها المورد، • استخدام تجهيزات تكنولوجيا المعلومات غير التي يوفرها المورد (مثل: جلب الجهاز الشخصي)، • استخدام أجهزة التخزين المحمولة/القابلة للإزالة، • المسؤوليات عند التعامل مع أصول معلومات بنك باركليز وحفظها وتخزينها؛ • ومخرجات قنوات تسريب البيانات؛ • والمخاطر والتبعات المترتبة على إساءة استخدام العناصر المذكورة أعلاه و/أو أي نتائج غير قانونية أو ضارة أو مسيئة ناجمة عن سوء الاستخدام هذا. يجب على المورّد اتخاذ الإجراءات المناسبة لضمان الالتزام بمتطلبات الاستخدام المقبول.	يساعد مطلب الاستخدام المقبول على تعزيز بيئة التحكم التي تحمي أصول المعلومات.
5. التثقيف والتوعية	يجب أن يكون لدى المورّد برنامج تدريبي للتثقيف والتوعية بالأمن يتم إنشاؤه لجميع الموظفين والمتعاقدين ومستخدمي أنظمة المؤسسة من الجهات الخارجية ويتم تقريره عند الاقتضاء. ويجب أن يتلقى جميع الأفراد الذين يحق لهم الوصول إلى بيانات/معلومات بنك باركليز تدريبًا مناسبًا خاصًا بالتثقيف والتوعية، بالإضافة إلى حصولهم على تحديثات منتظمة فيما يتعلق بالإجراءات والعمليات والسياسات التقنية والتنظيمية المرتبطة بوظيفتهم المهنية ذات الصلة بالمؤسسة. يجب أن تكون مستويات التثقيف والتدريب والتوعية متكافئة مع الأدوار المضطلع بها والمسجَّلة في منصة إدارة التعلُّم المناسبة. يجب على المورّد التأكُّد من أنَّ جميع الأفراد العاملين تحت سيطرته يخضعون لتدريب إلزامي يتعلق بمعلومات الأمن (تُحدَّث المعلومات باستمرار للتعويض عن التهديدات المتنامية والمخاطر الخاصة بالصناعة)، ويتضمن هذا التدريب	يدعم التعليم والتثقيف كل الضوابط الأخرى ضمن هذا الجدول الزمني. إذا لم يتم تنفيذ هذا المبدأ، فلن يكون الموظفون المعنيون على دراية بالأخطار السيبرانية وناقلات الهجوم ولن يكونوا قادرين على اكتشاف الهجمات أو منعها.

	أفضل ممارسات الأمن السيبراني وحماية بيانات بنك باركليز في غضون شهر واحد من الانضمام إلى المؤسسة؛ ويخضع التدريب للتحديث سنويًا على الأقل. وينبغي تضمين ما يأتي عند الاقتضاء: ينبغي أن تتلقى المجموعات التي تنطوي على خطورة عالية، مثل: المجموعات التي تتمتع بامتياز الوصول أو التي تعمل في وظائف تجارية حسَّاسة (بما في ذلك المستخدمون المتميزون وكبار المسؤولين التنفيذيين والأفراد العاملون في مجال أمن المعلومات والأمن السيبراني وأصحاب المصلحة من الأطراف الثالثة)، تدريبًا معزَّزًا للتوعية بالمواقف ذات الصلة بأمن المعلومات والأمن السيبراني وفقًا لأدوارهم ومسؤولياتهم. ينبغي تقديم هذا التدريب من خلال خبراء خارجيين تابعين لأطراف ثالثة، عند الاقتضاء.	
6. إدارة الحوادث الأمنية	يجب على المورّد إنشاء إطار عمل لإدارة الحوادث الأمنية، ويتحقَّق هذا الإطار بفاعلية من الحوادث الأمنية الناتجة عن بيئة المورّد، ويعمل على تصعيدها بكفاءة واحتوائها ومعالجتها. يجب على المورّد التأكُّد من وجود خطط مكتوبة مصممة خصوصًا للاستجابة للحوادث لكل فئة من فئات المخاطر/الحوادث الأمنية المعروفة التي تُحدِّد أدوار الأفراد العاملين وآليات التصعيد ومراحل معالجة/إدارة الحوادث: • التحقُّق من الحوادث - إنشاء عملية تحقُّق من الحوادث تستفيد من مختلف مصادر البيانات وتكون متكاملة عبر المؤسسة للتحقُّق بفاعلية من أحد الحوادث الأمنية (يعتمد هذا الأمر على أنَّ المورّد لديه آليات مراقبة واكتشاف فعَّالة وملائمة في جميع أنحاء بيئة تكنولوجيا المعلومات). • تصنيف الحوادث - إنشاء عملية تصنيف للحوادث تصنِّف الحادث الذي تم التحقُّق منه بسرعة وفاعلية عبر جميع أنواع الأحداث. • تصعيد الأحداث - إنشاء آليات مناسبة لتصعيد الحادث (حسب التصنيف) إلى أصحاب المصلحة المناسبين والأفراد الخاضعين للمساءلة والمتخصصين الخارجيين عند الاقتضاء، ما يؤدي إلى تمكين أنشطة الاستجابة السريعة للحوادث. • احتواء الحوادث - الاستفادة من القدرات البشرية والعملية والتكنولوجية لتحديد متجه الهجوم بسرعة وفاعلية واحتواء الحوادث الأمنية داخل البيئة وفقًا لذلك. • المعالجة - الاستفادة من القدرات البشرية والعملية والتكنولوجية لمعالجة أي تهديد أمني و/أو مكوّناته من البيئة بسرعة وفاعلية. ستضمن المعالجة الفعَّالة ضد الهجمات ذات الطبيعة المشابهة في المستقبل. ينبغي أن يسعى المورّد إلى إثبات تحسين أنشطة الاستجابة للحوادث حيثما أمكن من خلال دمج الدروس المستفادة من أنشطة الكشف/الاستجابة الحالية والسابقة. ينبغي للمورّد التأكُّد من اختبار فرق الاستجابة للحوادث وعملياتها، مرة واحدة سنويًا على الأقل، لضمان قدرته على الاستجابة لحوادث الأمن السيبراني. • يجب أن تُثبِت عمليات المحاكاة والاختبارات أنَّ بنك باركليز سيتم إخطاره بالحوادث الأمنية التي تؤثر فيه؛ وسيتضح ذلك من خلال إظهار المورّد قدرته على الاتصال بالأشخاص المناسبين في حالة وقوع مثل هذه الحوادث. • الاتصال - يجب على المورّد تعيين نقطة اتصال تخص أي حوادث أمنية وتتمثَّل مهمتها في التواصل مع بنك باركليز في حالة وقوع حادث ما. ينبغي للمورّد إخطار بنك باركليز بتفاصيل الاتصال بالفرد (الأفراد) وأي تغييرات تطرأ عليها، بما في ذلك أي جهات اتصال وأرقام هواتف خارج ساعات العمل.	تساعد عملية إدارة الحوادث والاستجابة لها على ضمان احتواء الحوادث بسرعة ومنع تصعيدها.

	ينبغي أن تتضمن التفاصيل ما يأتي: الاسم والمسؤوليات داخل المؤسسة والدور وعنوان البريد الإلكتروني ورقم الهاتف سيُبلغ المورّد بنك باركليز، في غضون إطار زمني معقول، فور علمه بأي حادث يؤثر في الخدمة المقدَّمة إلى بنك باركليز أو إلى معلومات/بيانات بنك باركليز، وفي كل الأحوال، في موعد لا يتجاوز **ساعتين (2)** من وقت علم المورّد بالحادث. في حالة وجود انتهاك مشتبه فيه أو معلوم في البيانات (بما في ذلك انتهاك الأمان الذي يؤدي إلى تدمير عرضي أو غير قانوني للبيانات الشخصية أو فقدانها أو تعديلها أو الكشف غير المصرَّح لها أو الوصول إليها)، يجب على المورّد إعلام بنك باركليز بهذه الحوادث ضمن إطار زمني معقول عندما يصبح على علم بأي من هذه الحوادث، وعلى أي حال، في موعد لا يتجاوز **ساعتين** من وقت علم المورّد بمثل هذه الحوادث. بالإضافة إلى الإخطار المبدئي على النحو المفصَّل أعلاه، سيُقدِّم المورّد تقريرًا إلى بنك باركليز في غضون **24 ساعة** من علمه بأي حادث يؤثر في الخدمة المُقدَّمة إلى بنك باركليز أو معلومات/بيانات بنك باركليز. ينبغي أن يتضمن التقرير التفاصيل الآتية: • التاريخ والوقت اللذان علم المورّد فيهما بالحادث الأمني • دوائر الاختصاص القضائي المتأثرة المشتبه فيها • نوع الحادث الأمني وملخص موجز له • التأثير والتبعات المحتملة على الخدمات المُقدَّمة إلى بنك باركليز و/أو معلومات/بيانات بنك باركليز (وأصحاب البيانات المتأثرة إذا أمكن ذلك) • حالة الحادث الأمني (على سبيل المثال، تعيين خبراء الطب الشرعي، وإخطار السلطات المعنية، ومعرفة ناقل الهجوم، وتحسين المراقبة الموجودة، وتطبيق الاحتواء) • الإجراءات المُتخذة أو المخطط لها لمعالجة الحادث الأمني • تفاصيل أي بيانات مخترَقة ينبغي إبلاغ مدير المورّدين في بنك باركليز ومركز العمليات المشتركة في بنك باركليز ضمن **مركز العمليات المشتركة بمكتب الأمن الرئيس في بنك باركليز** gcsojoc@barclays.com بهذه الحوادث، بالإضافة إلى جميع التحديثات الجارية ذات الصلة بجهود المعالجة والإعلامات المُرسلة إلى أصحاب البيانات. **يرجى ملء موضوع رسالة البريد الإلكتروني "[إدراج اسم المورّد] – الحادث الأمني – العناية العاجلة مطلوبة". إذا كان الحادث عاجلاً للغاية ويلزم الإبلاغ عنه على الفور، فمن الممكن الوصول إلى مركز العمليات المشتركة على مدار اليوم وطوال أيام الأسبوع على الخط الساخن الآتي:** • المملكة المتحدة: +44 330 041 5586 • الولايات المتحدة: +1 201 499 1900 • الهند: +91 788 781 9890	

7. تصنيف المعلومات وحمايتها	يجب أن يكون لدى المورّد إطار عمل/مخطط قائم ومناسب لتصنيف المعلومات ومعالجتها وتخزينها (بما يتوافق مع أفضل ممارسة في الصناعة و/أو متطلبات بنك باركليز)، ويتضمن — على سبيل المثال لا الحصر — المكوّنات الآتية: • مراجعة المعلومات/البيانات الحالية والجديدة المتعلقة ببنك باركليز باستمرار • تعيين مخطط تسمية المعلومات الصحيحة لمعلومات/بيانات بنك باركليز. • معالجة معلومات/بيانات بنك باركليز وتخزينها بشكل آمن ومناسب، بما يتماشى مع مستوى التصنيف المعيَّن لها. • التأكُّد من أنَّ جميع الموظفين على دراية بمتطلبات التسمية والتخزين والمعالجة الخاصة بالمورّد/بنك باركليز، وكيفية تطبيق تصنيف المعلومات الصحيح. يجب على المورّد الرجوع إلى مخطط التسميات المعلوماتية ومتطلبات المعالجة من بنك باركليز (الملحق B، الجدول B1 و(B2، أو مخطط بديل لضمان أن يقوم المورّد بحماية معلومات بنك باركليز المحفوظة و/أو المعالجة وتأمينها. ينطبق هذا المطلب على جميع أصول المعلومات المحفوظة أو المعَالجة نيابة عن بنك باركليز.	إذا لم يتم تنفيذ هذه المتطلبات، فقد يؤدي ذلك إلى أن تصبح بيانات بنك باركليز عرضة للتعديل أو الكشف أو الوصول أو الضرر أو الفقدان أو التدمير غير المصرَّح به، وهو الأمر الذي قد يترتب عليه ضرر تنظيمي وإضرار بالسمعة.
8. إدارة أصول تكنولوجيا المعلومات (الأجهزة والبرامج)	يجب على المورّد التأكُّد من إنشاء برنامج فعَّال لإدارة الأصول طوال دورة حياتها. وينبغي أن تحكم إدارة الأصول دورة حياتها بداية من الاستحواذ إلى النفاد، مع توفير الرؤية والأمن لكل فئات الأصول في البيئة. يجب على المورّد الاحتفاظ بقائمة جرد كاملة ودقيقة من الأصول التجارية المهمة الموجودة في كل المنصات و/أو المواقع الجغرافية التي تقدِّم الخدمة (الخدمات) إلى بنك باركليز، بما في ذلك أي معدات تخص بنك باركليز تستضيفها أماكن العمل التابعة للمورّد و/أو المتعاقد معه من الباطن مقدمة من بنك باركليز، مع التأكُّد من إجراء اختبار واحد على الأقل سنويًا للتحقُّق من أنَّ قائمة جرد الأصول قائمة وكاملة ودقيقة. وبحد أدنى، ينبغي أن تتناول عملية إدارة الأصول الجوانب الآتية: • يتم تعيين/تحديث جميع أصول المعلومات والبنية التحتية باستمرار. • بعد ذلك، تتم حماية أصول المعلومات والبنية التحتية حسب تصنيفها وأهميتها وقيمتها التجارية. • يجب أن تكون لدى المورّد ضوابط مطبَّقة تضمن التسجيل والصيانة المستمرة لبيانات أصول الأجهزة طوال دورة حياة الأصول. • يجب على المورّد الاحتفاظ بقائمة جرد محدَّثة من الأصول • **يجب أن يحتفظ المورّدون الذين لديهم إعداد من المستوى 1 والمستوى 2 والمستوى 3 بقوائم جرد قائمة وكاملة ودقيقة من الأصول (بما في ذلك، جميع نقاط النهاية و/أو أجهزة الشبكة و/أو رموز RSA المميَّزة و/أو أي أصول مقدَّمة من بنك باركليز).** • **يجب على المورّد إجراء تسوية لجميع أصول بنك باركليز (الأجهزة والبرامج) على أساس سنوي، وتقديم شهادة تصديق إلى بنك باركليز (مكتب الأمن الرئيس - فريق ECAM).** • التأكُّد من إزالة الأصول غير المصرَّح بها من الشبكة أو عزلها، وتحديث قائمة الجرد في الوقت المناسب. • الاحتفاظ بقائمة محدَّثة لجميع البرامج المصرَّح بها والمطلوبة لتقديم خدمة بنك باركليز. • ضمان الاكتفاء بإضافة تطبيقات البرامج أو أنظمة التشغيل المدعومة حاليًا وتحديثات البائع المستلمَة فقط إلى قائمة جرد برامج المؤسسة المصرح بها. يجب وضع علامة على البرامج غير المدعومة لتدل على أنها غير	يعد الجرد الكامل والدقيق لأصول المعلومات ضروريًا لضمان الضوابط المناسبة. إذا لم يتم تنفيذ هذا المبدأ، فقد تقع أصول بنك باركليز أو الأصول التي يستخدمها الموردون لخدمة بنك باركليز عرضة للأخطار، ما قد يسفر عن خسائر مالية وضياع للبيانات وإضرار بالسمعة وإدانة تنظيمية.

	مدعومة في نظام الجرد. ينبغي أيضًا وضع علامة على البرامج التي تقترب صلاحيتها على الانتهاء على هذا النحو في نظام الجرد. ينبغي للمورّد ضمان تنفيذ إجراءات فعَّالة ومؤثرة في الوقت المناسب لتخفيف استخدام التكنولوجيات غير المدعومة ونهاية العمر الافتراضي للأصول والبيانات ونفادها وإتلافها للتخلص من أخطار اختراق البيانات.	
9. تدمير/التخلص من الأصول المادية والبيانات المتبقية من المعلومات الإلكترونية	يجب أن يتم تدمير أصول معلومات بنك باركليز، المخزَّنة إما في صيغة مادية أو إلكترونية، أو محوها بطريقة آمنة مناسبة للمخاطر المرتبطة بها، ما يضمن عدم إمكانية استرداد بيانات بنك باركليز. ينبغي للمورّد تطبيق سياسات وإجراءات فعَّالة لتقييم — وتحديد باستمرار — متى يكون تدمير أصول معلومات بنك باركليز المخزَّنة إما بصيغة مادية أو إلكترونية، أو حذفها، أمرًا مناسبًا ومطلوبًا، حسب العقد أو لأغراض قانونية أو تنظيمية أو تتعلق بأمن المعلومات. قد يسعى بنك باركليز أيضًا إلى تدمير أصول المعلومات لديه، وذلك من خلال طلب مكتوب. ينبغي للمورّد وضع إجراءات إلى جانب عمليات تجارية داعمة وتدابير تقنية يتم تنفيذها للتخلص الآمن من بيانات بنك باركليز (بما في ذلك النُّسخ الاحتياطية) وإزالتها/محوها بأمان من جميع وسائط التخزين، وهذا ما يضمن عدم استرداد البيانات بأي من وسائل الطلب الشرعي الحاسوبي. يجب مسح بيانات بنك باركليز المخزَّنة في الوسائط حتى الوصول إلى مستوى كاف، بحيث لا يمكن استرداد البيانات، ويُفضَّل استخدام تقنيات مناسبة لمحو البيانات، مثل: المسح الآمن أو الإزالة أو محو البيانات أو تدمير البيانات أو الطريقة المستندة إلى البرامج لاستبدال البيانات أو استخدام إطار العمل القياسي للصناعة الخاص بالتخلص من البيانات (NIST). يجب التخلص من جميع المعلومات في نهاية عمرها التشغيلي (من بينها المعدات المعيبة، والمعدات التي توقف تشغيلها بسبب الصيانة، والمعدات التي خرجت من الخدمة ولم تعد مطلوبة، والمعدات المستخدمة في التجارب أو إثبات صحة أحد المفاهيم، وما إلى ذلك). يمكن الاستفادة من خدمات محو البيانات في المعدات التي سيُعاد استخدامها. تسري متطلبات التخلص على الأطراف الرابعة من المورّدين/الوكالات المتعاقد معها من الباطن التي تمت الاستعانة بها لتقديم الخدمة إلى بنك باركليز. عند التخلص من النسخ الورقية من المعلومات، لا بد من تمزيقها حتى الوصول إلى الحد الأدنى من معيار P4 DIN66399، وذلك باستخدام أداة سحق الورق (يتضمن هذا معلومات بطاقة الدفع)، أو يمكن حرقها امتثالاً لـ BS EN15713:2009. بالنسبة إلى بنك باركليز، يجب الاحتفاظ بدليل التخلص من البيانات، مع توفير مسار للمراجعة وأدلة ووسائل تعقُّب، وينبغي أن تتضمن ما يأتي: • إثبات التدمير و/أو التخلص (بما في ذلك تاريخ التنفيذ والطريقة المستخدمة). • سجلات تدقيق النظام المطلوب حذفها. • شهادات التخلص من البيانات. • الأفراد الذين قاموا بعملية التخلص (بما في ذلك، أي شركاء أو أطراف ثالثة أو متعاقدين شاركوا في عملية التخلص) • يجب إنشاء تقرير يخص التدمير والتحقُّق للتأكيد على نجاح أي عملية تدمير/حذف أو فشلها (على سبيل المثال: يجب تقديم تقرير من عملية الاستبدال يتناول بالتفصيل أي قطاعات تعذر محوها).	يساعد الإتلاف الآمن لأصول المعلومات على ضمان استحالة استرداد أصول معلومات بنك باركليز لإحداث أي انتهاك للبيانات أو ضياعها أو أي نشاط ضار يتعلق بها.

	في أثناء الإنهاء، يجب على المورّد التأكّد من تدمير بيانات بنك باركليز بأمان بناءً على إخطار وتفويض من بنك باركليز.	
10. أمن الحدود والشبكات	يجب على المورّد التأكُّد من أنَّ جميع أنظمة تكنولوجيا المعلومات، التي يديرها هو أو المتعاقد معه من الباطن والتي تدعم الخدمة (الخدمات) المقدَّمة إلى بنك باركليز، محمية من تهديدات الشبكة الواردة والصادرة داخل شبكة المورّدين (وأي متعاقدين من الباطن ذوي صلة). تجب على المورّد مراقبة تدفق المعلومات المنقولة عبر الشبكات ذات مستويات الثقة المختلفة مع التركيز على الانتهاكات الأمنية، والكشف عنه ومنعه ومعالجته إذا لزم الأمر. ينبغي أن تتضمن آليات سلامة الشبكة، على سبيل المثال لا الحصر، المجالات الآتية: • الاحتفاظ بقائمة جرد محدَّثة لجميع حدود شبكة المؤسسة (من خلال بنية الشبكة/الرسم التخطيطي الخاص بها). • تجب مراجعة تصميم الشبكة وتنفيذها، بالإضافة إلى نقاط الضعف المحتملة والحاجة إلى توقف البنية التحتية للشبكة وتجديدها، مرة واحدة سنويًا على الأقل أو في حالة وجود مطلب مدفوع بالأحداث يؤدي إلى إجراء تغييرات. • يتم توثيق الاتصالات الخارجية بشبكة المورّدين وتوجيهها من خلال جدار الحماية والتحقُّق منها والموافقة عليها قبل إنشاء الاتصالات لمنع الانتهاكات الأمنية. • تتم حماية شبكات المورّدين من خلال تطبيق مبادئ دفاعية متعمقة (مثل: تجزئة الشبكة، وجدران الحماية، وضوابط الوصول المادي إلى تجهيزات الشبكة، وما إلى ذلك). • يلزم أن تكون لدى المورد تكنولوجيات لمنع اختراق الشبكات بهدف اكتشاف حركات المرور الضارة ومنعها من الدخول إلى الشبكة. • استخدام قدرات جدران حماية الشبكة القوية لتوفير طبقة دفاع محيطي ضد هجمات الشبكة الضارة. • ينبغي أن تمر حركة المرور في شبكة الإنترنت من خلال وكيل يتم تكوينه لتصفية الاتصالات غير المصرَّح بها. • التأكد من ضرورة تمكين التسجيل والمراقبة. • تتم تقوية أجهزة الشبكة بأمان لمنع أي هجوم ضار. • الفصل المنطقي لمنافذ/واجهات إدارة الأجهزة عن حركة مرور المستخدم، ضوابط المصادقة المناسبة. • يلزم توثيق جميع قواعد التكوين التي تسمح بتدفق حركة المرور عبر أجهزة الشبكة في نظام إدارة التكوين مع وجود سبب تجاري محدد لكل قاعدة. • رفض الاتصال عبر منافذ بروتوكول التحكم في النقل (TCP) أو بروتوكول حزم بيانات المستخدم (UDP) غير المصرح بها أو حركة مرور التطبيقات لضمان حصر السماح بعبور حدود الشبكة دخولاً إليها أو خروجًا منها عند كل حد من حدود شبكة المؤسسة على البروتوكولات المعتمدة فقط. • إجراء عمليات مسح منتظمة من خارج كل حد من حدود الشبكة الموثوق بها لاكتشاف أي اتصالات غير مصرح بها يمكن الوصول إليها عبر الحدود. • تأمين الاتصالات بين الأجهزة ومحطات/وحدات التحكم بالإدارة. • تكوين أنظمة مراقبة لتسجيل حزم الشبكات التي تعبر الحدود عند كل حد من حدود شبكة المؤسسة.	إذا لم يتم تنفيذ هذا المبدأ، فقد تتعرَّض الشبكات الخارجية أو الداخلية للإفساد من جانب المهاجمين بهدف الوصول إلى الخدمة أو البيانات الموجودة داخلها.

	• يلزم تشفير اتصال الشبكة بين موفر الخدمة الداخلي/عبر السحابة/مراكز البيانات عبر بروتوكول آمن. يجب تشفير أصول معلومات/بيانات بنك باركليز التي يتم نقلها داخل شبكة المناطق الواسعة (WAN) إلى المورّدين. • يجب المورّد بمراجعة قواعد جدار الحماية (جدار الحماية الخارجي والداخلي) على أساس سنوي. • يخضع كل الوصول اللاسلكي إلى الشبكة لبروتوكولات التصريح والمصادقة والتجزئة والتشفير لمنع الانتهاكات الأمنية. • يجب على المورّد التأكُّد من ضرورة مراقبة الوصول إلى الشبكة الداخلية، وضرورة السماح بالأجهزة المصرَّح بها فقط من خلال الضوابط المناسبة للوصول إلى الشبكة. • يجب استخدام مصادقة متعددة العوامل عند الوصول عن بُعد إلى شبكة المورّد من خلال تسجيل الدخول. • يجب أن تكون لدى المورّد شبكة منفصلة للخدمة (الخدمات) المقدَّمة إلى بنك باركليز. يجب على المورّد التأكُّد من عدم نشر أي خوادم مستخدمة لتقديم الخدمة إلى بنك باركليز على شبكات غير موثوق بها (الشبكة التي تقع خارج محيط الأمن الخاص بك، وتكون خارجة عن سيطرتك الإدارية، مثل: واجهة الإنترنت) من دون ضوابط أمنية مناسبة. يجب على المورّد، الذي يستضيف معلومات بنك باركليز (بما في ذلك المتعاقدون من الباطن) في مركز البيانات أو السحابة، الحصول على شهادة أفضل ممارسة في الصناعة. - شبكات T2 وT3 • يجب إجراء فصل منطقي بين شبكة T2 وشبكة شركة المورّد باستخدام جدار الحماية، كما يجب تقييد حركة المرور الواردة والصادرة ومراقبتها. • يجب أن يقتصر ضمان تكوين التوجيه على الاتصالات بشبكة بنك باركليز فقط كما يجب عدم القيام بالتوجيه إلى أي شبكات أخرى للمورّدين. • يجب إجراء تكوين آمن لموجه الحافة الخاص بالمورّد والمتصل ببوابات الشبكة الخارجية لبنك باركليز باستخدام مفهوم الحد من ضوابط المنافذ والبروتوكولات والخدمات؛ ○ التأكد من ضرورة تمكين التسجيل والمراقبة. *ملحوظة. يشير مصطلح "الشبكة" كما هو مستخدم في عنصر التحكم هذا إلى أي شبكة غير تابعة لبنك باركليز يكون المورّد مسؤولاً عنها، بما في ذلك شبكة المتعاقد معه من الباطن.*	
11. اكتشاف حجب الخدمة	يلزم أن يحتفظ المورد بالقدرة على اكتشاف هجمات حجب الخدمة (DoS) وحجب الخدمة الموزعة (DDoS) والحماية منها. كما يلتزم المورد بالتأكد من أن القنوات المتصلة بالإنترنت أو القنوات الخارجية التي تدعم الخدمات المقدمة إلى بنك باركليز يجب أن تحظى بحماية كافية ضد هجمات DoS لضمان التوافر. إذا كان المورّد يستضيف تطبيقًا مواجهًا للإنترنت ويحمل أي بيانات مقيّدة أو يدعم خدمة من فئة المرونة 0 أو 1، فلا بد من حماية ذلك وصولاً إلى طبقة 7 باستخدام التقنيات المناسبة التي يجب أن يوافق عليها بنك باركليز.	إذا لم يتم تنفيذ هذا المبدأ، فقد يتعذر على بنك باركليز ومورّديه منع هجوم حجب الخدمة من تحقيق هدفه.

12. العمل عن بُعد (الوصول عن بُعد)	الوصول عن بُعد إلى شبكة بنك باركليز عبر تطبيقات Citrix الخاصة ببنك باركليز و/أو بيانات بنك باركليز الموجودة/المخزَّنة داخل البيئات/الشبكات التي يديرها المورّدون، إذا كان المورّد أو أي من المتعاقدين معه من الباطن يمكنهم الوصول إلى بيانات بنك باركليز أو البيانات الشخصية في بنك باركليز أو أي معلومات حسَّاسة تُقدَّم إلى المورّد على أساس الحاجة إلى المعرفة، سواء في صيغة مادية أم افتراضية، ليتم الوصول إليها أو مشاركتها أو معالجتها عن بُعد، وخاصة في الأماكن التي من الممكن أن يعمل فيها موظفو المورّد من المنزل، وسيطلب المورّد الحصول على موافقة مسبقة من بنك باركليز (مكتب الأمن الرئيس – فريق ECAM) لتهيئة هذه الترتيبات. لتحقيق الوصول عن بُعد، يجب على المورّد التأكُّد من إنشاء المكوّنات الآتية بحد أدنى: • يجب تشفير الوصول إلى شبكة المورّد عن بُعد بتسجيل الدخول في أثناء نقل البيانات واستخدام دومًا المصادقة متعددة العوامل. • يجب أن يكون الوصول إلى شبكة بنك باركليز عبر تطبيق Citrix الخاص ببنك باركليز باستخدام رمز التشفير باستخدام مفتاح عام (RSA) (الجهاز والبرنامج) المقدم من بنك باركليز. • يحافظ المورّد على جرد لجميع رموز التشفير باستخدام مفتاح عام (RSA) (الجهاز والبرنامج) المقدَّمة من بنك باركليز وعملية إدارة تتضمن مراجعة ورصد تخصيص الرموز (جهاز رموز الأمان) واستخدامها وإرجاعها. • يجب على المورد الاحتفاظ بسجلات للأفراد الذين طُلب منهم العمل عن بُعد والأسباب المنطقية وراء هذا المطلب • **يقوم المورد بإجراء تسوية لجميع المستخدمين عن بُعد على أساس ربع سنوي وتقديم شهادة تصديق إلى بنك باركليز (مكتب الأمن الرئيس - فريق ECAM)** • سيقوم بنك باركليز بإلغاء تنشيط بيانات اعتماد المصادقة على الفور في حال عدم استخدامها لفترة من الوقت (لا تتجاوز فترة عدم الاستخدام هذه شهرًا واحدًا). • يجب على المورّد التأكُّد من ضرورة تكوين نقطة النهاية المستخدمة لنقل أنظمة معلومات بنك باركليز عن بُعد بأمان ووفقًا أفضل ممارسة في الصناعة (على سبيل المثال، مستوى التصحيح، وحالة مكافحة البرامج الضارة، وحل EDR لاكتشاف نقاط النهاية والاستجابة لها، والتسجيل، وما إلى ذلك). • يجب اعتماد الخدمات التي تتمتع بإمكانية الوصول إلى الطباعة عن بُعد عبر تطبيق Citrix الخاص ببنك باركليز وترخيصها من قِبل بنك باركليز (مكتب الأمن الرئيس - فريق ECAM). يتعين على المورد الاحتفاظ بالسجلات وإجراء التسوية على أساس ربع سنوي. • **يجب عدم السماح للأجهزة الشخصية/جلب الجهاز الشخصي (BYOD) بالوصول إلى بيئة بنك باركليز و/أو بيانات بنك باركليز الموجودة/المخزنة في بيئة يديرها المورّد (التي تشمل، على سبيل المثال لا الحصر، موظفي المورّد والاستشاريين وعمال الطوارئ والمتعاقدين وشركاء الخدمة المدارة).** عند منح شبكة بنك باركليز حق الوصول إلى نقاط النهاية (جهاز كمبيوتر محمول/جهاز كمبيوتر مكتبي) من خلال تطبيقات Citrix الخاصة ببنك باركليز عبر الإنترنت، يجب على المورّد تثبيت أداة تحليل نقطة النهاية التي يوفّرها بنك باركليز للتحقُّق من أمان نقطة النهاية وامتثال نظام التشغيل، ولن يُمنح حق الوصول عن بُعد إلى شبكة بنك باركليز إلا للأجهزة التي تجتاز فحوصات تحليل نقطة النهاية من خلال تطبيق Citrix الخاصة ببنك باركليز. إذا تعذر على المورّد تثبيت أداة تحليل نقطة النهاية أو استخدامها، فلا بد من إخطار مدير المورّدين في بنك باركليز بذلك.	تساعد ضوابط الوصول عن بُعد على ضمان عدم اتصال الأجهزة غير المصرح لها وغير الآمنة ببيئة بنك باركليز عن بُعد.

<table>
<tr><td></td><td>ملحوظة: سيلغي بنك باركليز تنشيط بيانات اعتماد المصادقة عند الإخطار بأنه لم تعد هناك حاجة إلى الوصول (كأن يتم إنهاء عمل الموظف، إعادة تعيين المشروع، إلخ) في غضون أربع وعشرين (24) ساعة.</td><td></td></tr>
<tr><td>13. إدارة سجلات الأمان</td><td>يجب على المورّد التأكُّد من وجود إطار عمل قائم لإدارة التدقيق والتسجيل، وهذا الإطار سيؤكِّد على أنَّ أنظمة تكنولوجيا المعلومات الأساسية وعملياتها، بما في ذلك التطبيقات وأجهزة الشبكة وقواعد البيانات ونقاط النهاية وأجهزة الأمان والبنية التحتية والخوادم، تُنتج السجلات المطلوبة وفقًا لأفضل ممارسة في الصناعة وإرشاداتها. ينبغي للمورّد تأمين هذه السجلات بشكل مناسب والحفاظ عليها بشكل مركزي والاحتفاظ بها لفترة لا تقل عن 12 شهرًا أو على أساس الفئات المذكورة أدناه مع الاستخدام المنطقي الصحيح.
<table>
<tr><th>الفئة</th><th>أنظمة/خدمات منخفضة التأثير</th><th>أنظمة/خدمات متوسطة التأثير</th><th>أنظمة/خدمات عالية التأثير</th></tr>
<tr><td>الاحتفاظ بالسجلات</td><td>3 أشهر</td><td>6 أشهر</td><td>12 أشهر</td></tr>
</table>
وبحد أدنى، ينبغي أن تتناول عملية إدارة سجلات الأمان المجالات الآتية:

ينبغي للمورّد وضع سياسات وإجراءات لإدارة السجلات.
ينبغي للمورد إنشاء بنية تحتية لإدارة السجلات، وصيانتها.
ينبغي للمورد تحديد أدوار ومسؤوليات الأفراد والفرق المتوقع مشاركتهم في إدارة السجلات.
جمع سجلات التدقيق الخاصة بالأحداث من أجل المساعدة على مراقبة الهجوم أو الكشف عنه أو فهمه أو التعافي منه، وإدارتها وتحليلها.
تمكين تسجيل النظام لتضمين المعلومات التفصيلية، مثل: مصدر الحدث والتاريخ والمستخدم والطابع الزمني وعناوين المصدر وعناوين الوجهة وغيرها من العناصر الأخرى المفيدة.
قد تتضمن نماذج سجلات الأحداث ما يأتي:

نظام كشف التسلل (IDS)/نظام منع التسلل ((IPS، والموجه، وجدار الحماية، وملقم الويب، وبرنامج الوصول عن بُعد ((VPN، وخوادم التوثيق، والتطبيقات، وسجلات قاعدة البيانات.
عمليات تسجيل الدخول الناجحة، ومحاولات تسجيل الدخول الفاشلة (كمعرف المستخدم أو كلمة المرور الخاطئة)، وإنشاء حسابات المستخدمين وتعديلها وحذفها
سجلات تغيير التكوين.

خدمات بنك باركليز المتعلقة بتطبيقات الأعمال وأنظمة البنية التحتية التقنية التي يجب تمكين التسجيل المناسب والتسجيل حسب أفضل ممارسة في الصناعة عليها، بما في ذلك الأنظمة التي تتم الاستعانة بمصادر خارجية لتوفيرها أو "الموجودة في السحابة".
تحليل سجلات الأحداث المتعلقة بالأمن (ومنها التطبيع والتجميع والربط).
مزامنة الطوابع الزمنية في سجلات الأحداث على مصدر مشترك وموثوق
حماية سجلات الأحداث المتعلقة بالأمن (على سبيل المثال: عن طريق التشفير والمصادقة متعددة العوامل والتحكم في الوصول والنسخ الاحتياطي).
اتخاذ الإجراءات اللازمة لمعالجة أي مشكلات يتم تحديدها والاستجابة لحوادث الأمن السيبراني بطريقة سريعة وفعالة.
</td><td>إذا لم يتم تنفيذ هذا الضابط، فلن يتمكن المورّدون من اكتشاف الاستخدام غير الملائم أو الضار لخدمتهم أو بياناتهم والاستجابة له في غضون فترات زمنية معقولة.</td></tr>
</table>

	• نشر المعلومات الأمنية وإدارة الأحداث (SIEM) أو أدوات تحليل السجلات للربط بينها وتحليلها. • نشر الأدوات حسب الاقتضاء لإجراء تجميع مركزي في الوقت الفعلي والربط بين الأنشطة الشاذة، وتنبيهات الشبكة والنظام، والمعلومات الاستخباراتية المتعلقة بالأحداث والتهديدات السيبرانية ذات الصلة من مصادر متعددة التي من بينها المصادر الداخلية والخارجية على حد سواء، من أجل اكتشاف الهجمات السيبرانية متعددة الأوجه ومنعها بصورة أفضل. يلزم أن تتضمن الأحداث الرئيسة التي يتم تسجيلها الأحداث التي من المحتمل أن تؤثر في سرية الخدمات المقدمة إلى بنك باركليز وسلامتها ومدى توافرها، والتي قد تساعد على تحديد الحوادث المادية و/أو انتهاكات حقوق الوصول التي تحدث فيما يتعلق بأنظمة الموردين أو التحقيق فيها.	
14. التصدي للبرامج الضارة	تماشيًا مع أفضل ممارسة في الصناعة، يجب على المورّد وضع سياسات وإجراءات وتنفيذ عمليات تجارية وتدابير تقنية داعمة، لمنع تطبيق البرامج الضارة على بيئة تكنولوجيا المعلومات بأكملها. يجب على المورّد التأكُّد من تطبيق الحماية من البرامج الضارة على جميع أصول تكنولوجيا المعلومات المعمول بها طوال الوقت لمنع انقطاع الخدمة أو الانتهاكات الأمنية. ينبغي أن تتضمن الحماية من البرامج الضارة، على سبيل المثال لا الحصر، ما يأتي: • برامج لمكافحة البرامج الضارة تُدار مركزيًا للمراقبة المستمرة والدفاع عن بيئة تكنولوجيا المعلومات في المؤسسة. • التأكُّد من أنَّ برنامج مكافحة البرامج الضارة لدى المؤسسة يقوم بتحديث محرك الفحص الخاص به وقاعدة بيانات التوقيع على أساس منتظم ووفقَ أفضل ممارسة في الصناعة. • إرسال كل أحداث الكشف عن البرامج الضارة إلى أدوات إدارة مكافحة البرامج الضارة وخوادم سجلات الأحداث لدى المؤسسة للتحليل والتنبيه. • ينبغي للمورد تنفيذ الضوابط المناسبة للحماية من البرامج الضارة والهجمات على الأجهزة المحمولة المتصلة بشبكات بنك باركليز أو المورد التي يمكنها الوصول إلى بيانات بنك باركليز. • ينبغي تنفيذ العمليات للاجتماعات/المنتديات المنتظمة (على أساس شهري مثلاً) لمناقشة نقاط الضعف/التحديثات المحتملة المطلوبة. ينبغي اتخاذ إجراء المعالجة بطريقة مرتَّبة حسب الأولوية وفي الوقت المناسب. ينبغي الاحتفاظ بسجلات التقارير والمنتديات والإجراءات التصحيحية المتخذة. ملحوظة: تشمل مكافحة البرامج الضارة (على سبيل المثال لا الحصر) اكتشاف التعليمات البرمجية المتنقلة غير المصرح بها، والفيروسات، وبرامج التجسس، وبرامج رصد لوحة المفاتيح، وشبكة الروبوت، والفيروسات المتنقلة، وأحصنة طروادة، وغيرها.	تعد حلول مكافحة البرامج الضارة من ضرورات حماية أصول معلومات بنك باركليز من التعليمات البرمجية الضارة.
15. معايير التكوين الآمن	يلزم أن يكون لدى المورّد إطار عمل قائم لضمان تكوين جميع الأنظمة القابلة للتكوين/تجهيزات الشبكات بشكل آمن وفق أفضل ممارسة في الصناعة (مثل المعايير الخاصة بالمعهد الوطني للمعايير والتقنية (NIST) ومعهد سانس (SANS) ومركز أمن الإنترنت (CIS)). ينبغي أن يغطي معيار التكوين، على سبيل المثال لا الحصر، المجالات الآتية: • وضع السياسات والإجراءات/التدابير التنظيمية والأدوات اللازمة للسماح بتنفيذ معايير تكوين الأمن وفقَ أفضل ممارسة في الصناعة لجميع أجهزة الشبكة وأنظمة التشغيل والتطبيقات والخوادم المعتمدة.	تساعد ضوابط الإنشاء القياسية على حماية أصول المعلومات من الوصول غير المصرح به. كما يساعد الالتزام بالإنشاءات والضوابط القياسية التي تضمن السماح باعتماد التغييرات على ضمان حماية أصول معلومات بنك باركليز

	• إجراء فحوصات إنفاذ منتظمة (على أساس سنوي) لضمان التصحيح الفوري لعدم الامتثال لمعايير الأمن الأساسية. تطبيق عمليات فحص ومراقبة مناسبة لضمان الحفاظ على سلامة الإنشاءات/الأجهزة. • يتم تكوين الأنظمة وأجهزة الشبكة للعمل وفقَ مبادئ الأمن (مثل: مفهوم تقييد ضوابط المنافذ والبروتوكولات والخدمات، وعدم وجود برامج غير مصرح بها، وإزالة حسابات المستخدم غير الضرورية وتعطيلها، وتغيير كلمات مرور الحسابات الافتراضية، وإزالة البرامج غير الضرورية، وما إلى ذلك). التأكُّد من أنَّ إدارة التكوين تحكم معايير التكوين الآمن عبر جميع فئات الأصول، وتكتشف تغييرات التهيئة أو الانحرافات وتنبه بها وتستجيب لها بفعالية.	
16. أمن نقطة النهاية	يجب على المورّد التأكُّد من أنَّ تقوية نقاط النهاية المستخدمة للوصول إلى شبكة بنك باركليز، أو الوصول إلى/معالجة أصول معلومات/بيانات بنك باركليز للحماية من أي هجمات من البرامج الضارة. يجب أن تكون أفضل الممارسات في الصناعة في مكانها، كما يجب أن يتضمن إنشاء أمان نقاط النهاية، على سبيل المثال لا الحصر، ما يأتي: • تشفير الأقراص. • تعطيل جميع البرامج/الخدمات/المنافذ غير المطلوبة. • تعطيل الوصول إلى حقوق الإدارة للمستخدم المحلي. • عدم السماح لموظفي المورّد بتغيير الإعدادات الأساسية مثل: حزمة الخدمة الافتراضية وقسم النظام والخدمات الافتراضية وما إلى ذلك. • يجب تعطيل منفذ USB لمنع نسخ بيانات بنك باركليز إلى الوسائط الخارجية • التحديث باستخدام أحدث توقيعات مكافحة الفيروسات وتصحيحات الأمان. • تقييد منع فقدان البيانات بعدم استخدام القص والنسخ واللصق وطباعة الشاشة مع بيانات بنك باركليز • يجب تعطيل الوصول إلى الطابعة، بصورة افتراضية. • ينبغي للمورّد تقييد القدرة على الوصول إلى مواقع الشبكات الاجتماعية وخدمات بريد الويب والمواقع بإمكانية تخزين المعلومات على الإنترنت كاستخدام google drive وDropbox وiCloud. • ينبغي تعطيل مشاركة/نقل أصول معلومات/بيانات بنك باركليز باستخدام أدوات/برامج المراسلة الفورية. • توافر القدرة والعمليات الخاصة باكتشاف البرامج غير المصرح بها التي يتم تحديدها بوصفها ضارة ومنع تثبيت البرامج غير المصرَّح بها. ملحوظة: ينبغي تعطيل الوسائط القابلة للإزالة/الأجهزة المحمولة بصورة افتراضية وتمكينها فقط للأسباب التجارية المشروعة. ينبغي أن يحتفظ المورد بصور أو قوالب آمنة لكل الأنظمة في المؤسسة بناءً على معايير التكوين المعتمدة للمؤسسة. وينبغي تصوير أي نشر لنظام جديد أو أي نظام موجود يتم اختراقه، باستخدام إحدى هذه الصور أو القوالب. عند منح شبكة بنك باركليز حق الوصول إلى نقاط النهاية (أجهزة كمبيوتر محمولة/أجهزة كمبيوتر مكتبية) من خلال تطبيق Citrix الخاصة ببنك باركليز عبر الإنترنت، يجب على المورّد تثبيت أداة تحليل نقطة النهاية التي يوفّرها بنك باركليز للتحقّق من أمان نقطة النهاية وامتثال نظام التشغيل، ولن يُمنح حق الوصول عن بُعد إلى شبكة بنك باركليز إلا للأجهزة التي تجتاز فحوصات تحليل نقطة النهاية من خلال تطبيقات Citrix الخاصة ببنك باركليز. إذا تعذر على المورّد تثبيت أداة تحليل نقطة النهاية أو استخدامها، فلا بد من إخطار مدير المورّدين في بنك باركليز بذلك.	إذا لم يتم تنفيذ هذا الضابط، فقد تكون نقاط النهاية والشبكة الخاصة ببنك باركليز والمورّد عرضة للهجمات السيبرانية.

	الأجهزة المحمولة المستخدمة في خدمات بنك باركليز - 1. يجب على المورّد التأكُّد من تطبيقه قدرات إدارة الأجهزة المحمولة (MDM) للتحكم في الأجهزة المحمولة التي يمكنها الوصول إلى و/أو تحتوي على معلومات بنك باركليز السرية وإدارتها بأمان طوال دورة الحياة، ما يقلل من مخاطر اختراق البيانات. 2. يجب أن يضمن المورد تنفيذ إمكانات قفل الجهاز المحمول ومسحه عن بُعد لحماية المعلومات في حال فقد الجهاز أو سرقته أو تعرضه للخطر. 3. تشفير بيانات الجهاز المحمول (بيانات بنك باركليز).	
17. منع تسرب البيانات	يلزم أن يكون لدى المورد إطار عمل قائم لضمان وجود حماية ضد تسرب البيانات غير المناسب لضمان أن تشمل الحماية قنوات تسرب البيانات الآتية (على سبيل المثال لا الحصر): • النقل غير المصرح به للمعلومات خارج الشبكة الداخلية/شبكة المورّد ○ البريد الإلكتروني ○ بوابة الإنترنت/الويب (بما في ذلك التخزين عبر الإنترنت والبريد الإلكتروني) ○ DNS • ضياع أصول معلومات بنك باركليز الموجودة على الوسائط الإلكترونية المحمولة (بما في ذلك المعلومات الإلكترونية الخاصة بأجهزة الكمبيوتر المحمولة والأجهزة المحمولة والوسائط المحمولة) أو سرقتها. • النقل غير المصرح به للمعلومات إلى الوسائط المحمولة. • تبادل المعلومات غير الآمن مع أطراف ثالثة (أطراف رابعة أو متعاقدون من الباطن). • طباعة المعلومات أو نسخها بشكل غير ملائم.	ينبغي تطبيق الضوابط اللازمة بشكل فعال لضمان اقتصار معلومات بنك باركليز على الأفراد المخول لهم الوصول إليها (السرية) وحماية تلك المعلومات من التغيير غير المصرح به (السلامة)، بالإضافة إلى إمكانية استرجاعها وتقديمها حال تم طلبها (التوافر). في حال عدم تنفيذ تلك المتطلبات كما ينبغي، فقد تصبح معلومات بنك باركليز الحساسة عرضة للتعديل أو الإفصاح أو الوصول أو الضياع أو الإتلاف غير المصرح به، الأمر الذي قد يترتب عليه تطبيق عقوبات قانونية وتنظيمية أو الإضرار بالسمعة أو خسارة الأعمال
18. أمان البيانات	يجب على المورّد التأكد من أنّ أصول معلومات/بيانات بنك باركليز الموجودة في عهدته/شبكته تتمتع بالأمان المناسب للبيانات الذي يتحقَّق من خلال مجموعة من تقنيات التشفير والوسائل الآمنة للوصول إلى البيانات وحماية السلامة ومنع فقدان البيانات. من المهم توخي العناية المناسبة للحد من الوصول إلى أصول معلومات/بيانات بنك باركليز، بما في ذلك البيانات الشخصية ولجعل ذلك الوصول آمنًا. ينبغي أن تتضمن ضوابط أمان البيانات، على سبيل المثال لا الحصر، المجالات الآتية: 1. يلتزم المورّد في جميع الأوقات بالامتثال لأي قوانين معمول بها لحماية البيانات، وجميع تلك القوانين. 2. ينبغي وضع السياسات والإجراءات، وتنفيذ العمليات التجارية/التدابير التنظيمية والتدابير التقنية الداعمة، من أجل جرد تدفقات البيانات الموجودة (بصورة دائمة أو مؤقتة) داخل تطبيقات الخدمة الموزعة جغرافيًا (المادية والافتراضية) ومكونات شبكة البنية التحتية وأنظمتها و/أو المكونات المشتركة مع جهات خارجية وتوثيقها والحفاظ عليها. 3. الاحتفاظ بقائمة جرد لجميع المعلومات الحسَّاسة/السريَّة (بيانات بنك باركليز) التي يقوم المورّد بتخزينها أو معالجتها أو نقلها. 4. وضع معيار تصنيف للبيانات لضمان تصنيف المعلومات الحساسة (أصول معلومات/بيانات بنك باركليز) وحمايتها بصورة مناسبة. 5. التأكُّد من تصنيف جميع بيانات بنك باركليز ووضع علامة عليها استنادًا إلى معيار تصنيف المعلومات وحمايتها.	

	6. حماية البيانات غير النشطة؛ a. وبحد أدنى، يتم تشفير البيانات غير النشطة لمنع استغلال المعلومات الحساسة من خلال الوصول غير المصرح به. 7. مراقبة نشاط قاعدة البيانات؛ a. مراقبة الوصول إلى قاعدة البيانات والنشاط وتسجيله لتحديد النشاط الضار بسرعة وفاعلية. 8. حماية البيانات المستخدمة؛ a. التأكُّد من التحكم في عرض المعلومات الحساسة واستخدامها عبر إمكانات إدارة الوصول للحماية من استغلال المعلومات الحساسة. b. استخدام تكنولوجيات إخفاء البيانات وتعتيمها لحماية البيانات الحساسة المستخدمة بفعالية من الكشف غير المقصود و/أو الاستغلال الضار. 9. حماية البيانات المتنقلة، a. الاستفادة من إمكانات التشفير القوية لضمان حماية البيانات في أثناء النقل. b. يتم عادة تشفير البيانات في أثناء النقل باستخدام تشفير النقل أو الحمولة (حقل مراسلة أو حقل انتقائي). تتضمن آليات تشفير النقل على سبيل المثال لا الحصر: • أمان طبقة النقل (باتباع أفضل ممارسة في الصناعة للتشفير الحديث، بما في ذلك استخدام/رفض البروتوكولات والشفرات) • الاتصال النفقي الآمن (حزمة بروتوكول الإنترنت الأمنية (IPsec)) • بروتوكول النقل الآمن (SSH) c. يلزم تكوين بروتوكولات أمن النقل لمنع التفاوض بشأن الخوارزميات الأضعف و/أو أطوال المفاتيح الأقصر، عندما تدعم كلتا نقطتي النهاية الخيار الأقوى. 10. النسخ الاحتياطي للبيانات – a. يجب وضع أحكام لضمان نسخ المعلومات احتياطيًا بصورة ملائمة ومن ثم استعادتها (ويمكن استعادتها في غضون فترة زمنية معقولة) بما يتوافق مع المتطلبات المتفق عليها مع بنك باركليز. b. تأكَّد من أنَّ النُّسخ الاحتياطية محمية بشكل صحيح عبر الأمن المادي أو التشفير عند تخزينها، وكذلك عند نقلها عبر الشبكة. يشمل ذلك النسخ الاحتياطية عن بعد والخدمات السحابية. c. تأكد من أن جميع بيانات بنك باركليز يتم نسخها احتياطيًا بصورة تلقائية على أساس منتظم.	
19. أمن برامج التطبيقات	يلتزم المورد باستحداث التطبيقات باستخدام ممارسات التشفير الآمنة وفي بيئة آمنة. عندما يستحدث المورّد تطبيقات ليستخدمها بنك باركليز أو تُستخدم لدعم الخدمة المقدمة إلى بنك باركليز، يجب عليه تأسيس إطار عمل للاستحداث الآمن لمنع الانتهاكات الأمنية ولتحديد الثغرات في التعليمة البرمجية ومعالجتها في أثناء عملية الاستحداث. ينبغي أن يتضمن أمان برامج التطبيق، على سبيل المثال لا الحصر، المجالات الآتية:	تساعد الضوابط التي تحمي استحداث التطبيقات على ضمان تأمين التطبيقات عند النشر.

	• يجب وضع معايير تشفير آمنة واعتمادها بما يتوافق مع أفضل ممارسة في الصناعة لمنع نقاط الضعف الأمنية وانقطاعات الخدمة التي تحمي في الوقت نفسه من الثغرات المعروفة المحتملة. • تأسيس ممارسات تشفير آمنة مناسبة للغة البرمجة. • يلزم إجراء جميع عمليات الاستحداث في بيئة غير إنتاجية. • الحفاظ على بيئات منفصلة للأنظمة الإنتاجية وغير الإنتاجية. يجب ألا يكون للمطورين وصول غير مراقب إلى بيئات الإنتاج. • الفصل بين مهمات البيئات الإنتاجية وغير الإنتاجية. • يجري استحداث الأنظمة بما يتوافق مع أفضل ممارسات الاستحداث الآمن في الصناعة (كاستخدام مشروع أمن تطبيق الويب المفتوح (OWASP)). • ينبغي تخزين التعليمة البرمجية بشكل آمن وخاضع لضمان الجودة. • تنبغي حماية التعليمة البرمجية بصورة ملائمة من التعديل غير المصرح به بمجرد توقيع الاختبار وتسليمه إلى الإنتاج. • استخدام مكوّنات الجهات الخارجية المحدَّثة والموثوقة فقط للبرنامج الذي يستحدثه المورّد. • تطبيق أدوات التحليل الثابتة والديناميكية للتحقق من الالتزام بممارسات التشفير الآمن. • يلتزم المورد بضمان عدم استخدام البيانات الحية (ومنها البيانات الشخصية) في البيئات غير الإنتاجية. • يجب تصميم واجهات التطبيقات والبرامج (API) واستحداثها ونشرها واختبارها وفق أفضل ممارسة في الصناعة (مثل: OWASP لتطبيقات الويب). ينبغي للمورّد حماية تطبيقات الويب بنشر جدران حماية تطبيقات الويب (WAF) التي تفحص جميع حركات المرور المتدفقة إلى تطبيق الويب لرصد هجمات تطبيقات الويب الحالية والشائعة. بالنسبة إلى التطبيقات غير المستندة إلى الويب، يجب نشر جدران حماية خاصة للتطبيقات إذا كانت هذه الأدوات متاحة لنوع التطبيق المحدد. إذا تم تشفير حركة المرور، فينبغي إما إبقاء الجهاز محكومًا بالتشفير أو أن يتمكن من فك تشفير حركة المرور قبل التحليل. إذا لم يكن أي من الخيارين مناسبًا، فسيلزم نشر جدار حماية تطبيق الويب المستند إلى المضيف.	
20. إدارة الوصول المنطقي (LAM)	يلزم تقييد الوصول إلى المعلومات، مع مراعاة مبادئ الحاجة إلى المعرفة، وأقل امتياز، والفصل بين المهام. يتحمل مالك أصول المعلومات مسؤولية تحديد من يحتاج إلى أي وصول.	تساعد ضوابط LAM المناسبة على ضمان حماية أصول المعلومات من الاستخدام غير المناسب. تساعد ضوابط إدارة الوصول على التأكُّد من أنَّ الوصول إلى أصول المعلومات غير متاح سوى للمستخدمين الذين تمت الموافقة عليهم.

	• ينص مبدأ الحاجة إلى المعرفة على وجوب تقييد وصول الأشخاص بالمعلومات التي يحتاجون إلى معرفتها فقط من أجل أداء مهامهم المصرح بها. فإذا كان الموظف على سبيل المثال يتعامل بصورة حصرية مع زبائن مقيمين في المملكة المتحدة، فلن "يحتاج إلى معرفة" المعلومات المتعلقة بالزبائن المقيمين في الولايات المتحدة. • وينص مبدأ أقل امتياز على وجوب حصول الأشخاص على الحد الأدنى فقط من الامتياز اللازم لأداء مهامهم المصرح بها. فإذا كان الموظف على سبيل المثال يحتاج إلى رؤية عنوان الزبون دون أن يكون مطالبًا بتغييره، فسيكون "أقل امتياز" يمكنه طلبه هو حق الوصول إلى القراءة فقط، الذي يلزم منحه إياه بدلاً من الوصول إلى القراءة/الكتابة. • ويتمثل مبدأ الفصل بين الواجبات في أن يكون شخصان على الأقل مسؤولَين عن الأجزاء المنفصلة لأي مهمة من أجل منع الخطأ والاحتيال. فيلزم ألا يكون الموظف الذي يطلب إنشاء الحساب على سبيل المثال هو نفسه الشخص الذي يوافق على الطلب. يجب على المورّد التأكُّد من إدارة الوصول إلى المعلومات الشخصية بشكل مناسب، وأن يقتصر على أولئك الذين يلزمهم الوصول من أجل تقديم الخدمة. ينبغي تحديد عمليات إدارة الوصول وفق أفضل ممارسة في الصناعة، وتشمل ما يأتي: • ينبغي للمورّد التأكُّد من توثيق عمليات إدارة الوصول إلى القرارات المتعلقة بها مع تطبيقها على جميع أنظمة تكنولوجيا المعلومات (التي تُخزّن أصول معلومات بنك باركليز)، وعند تنفيذ ذلك ينبغي توفير الضوابط الملائمة اللازمة لكل من: الملتحق/المنتقل/المغادر/الوصول عن بُعد. • يجب الالتزام بالضوابط المعمول بها في التفويض من أجل ضمان تكافئ عمليات منح الوصول وتعديله وإلغاءه المشتملة على مستويات من التفويض مع الامتيازات التي تم منحها. • يجب الالتزام بالضوابط المعمول بها للتأكُّد من اشتمال عمليات إدارة الوصول على الآليات اللازمة للتحقق من الهوية. • يجب ربط كل حساب بفرد واحد، يكون مسؤولاً عن أي نشاط يتم تنفيذه باستخدام الحساب. • إعادة اعتماد الوصول - يلزم تطبيق الضوابط لضمان مراجعة تصريحات الوصول كل 12 شهرًا على الأقل، وذلك من أجل ضمان مدى توافقها مع الغرض منها. • ينبغي مراجعة كافة تصاريح الوصول المميز كل ستة (6) أشهر على الأقل, فضلاً عن تطبيق الضوابط الملائمة لمتطلبات الوصول المميز. • ضوابط المنتقل - تم تعديل الوصول في غضون 24 ساعة من تاريخ النقل (والسجلات المناسبة المطلوب الاحتفاظ بها)؛ • ضوابط المغادر - تمت إزالة جميع عمليات الوصول المنطقية المستخدمة لتوفير الخدمات لبنك باركليز في غضون 24 ساعة من تاريخ المغادرة (والسجلات المناسبة المطلوب الاحتفاظ بها)، • الوصول عن بعد - ينبغي السماح بتطبيق ضوابط الوصول عن بعد فقط عبر آليات معتمدة من قِبل بنك باركليز (مكتب الأمن الرئيس - فريق ECAM) كما يلزم أن يستخدم الوصول عن بعد المصادقة متعددة العوامل. • المصادقة - يلزم اتباع طول كلمة المرور ودرجة تعقيدها المناسبَين أو تكرار تغيير كلمات المرور أو المصادقة متعددة العوامل أو الإدارة الآمنة لبيانات اعتماد كلمة المرور أو غيرها من الضوابط الأخرى وفق أفضل ممارسة في الصناعة.	

<table>
<tr>
<td></td>
<td>

الحسابات غير النشطة - ينبغي تعليق/تعطيل الحسابات غير المستخدمة لمدة 60 يومًا متتالية أو أكثر (والسجلات المناسبة المطلوب الاحتفاظ بها).
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.
ينبغي تغيير الحسابات المميَّزة بعد كل استخدام، وكل 90 يومًا بحد أدنى.
ينبغي تعطيل الحسابات التفاعلية بعد خمس محاولات فاشلة متتالية كحد أقصى أو حد أقصى أقل، في حالة فرض أفضل ممارسة في الصناعة.

</td>
<td></td>
</tr>
<tr>
<td>21. إدارة نقاط الضعف</td>
<td>
يجب على المورّد وضع سياسات وإجراءات،وتطبيق عمليات/تدابير تنظيمية داعمة، وتنفيذ تدابير تقنية، وذلك لإجراء مراقبة فعَّالة والكشف في الوقت المناسب عن نقاط الضعف الموجودة داخل التطبيقات والبنية التحتية ومكوّنات النظام المملوكة للمورّد أو التي يديرها المورّد، ومعالجتها، للتأكُّد من فاعلية الضوابط الأمنية التي يتم تنفيذها.

ينبغي أن تتضمن إدارة نقاط الضعف، على سبيل المثال لا الحصر، المجالات الآتية:

الأدوار والمسؤوليات وأوجه المساءلة المحدَّدة للمراقبة والإبلاغ والتصعيد والمعالجة.
الأدوات والبنية التحتية المناسبة لمسح الثغرات.
إجراء عمليات فحص لنقاط الضعف بصفة روتينية (بانتظام مثلما تفرضه أفضل ممارسة في الصناعة)، وتُحدِّد هذه العمليات نقاط الضعف المعروفة والمجهولة بفاعلية عبر جميع فئات الأصول داخل البيئة.
الاستفادة من عملية تصنيف المخاطر لتحديد أولويات معالجة نقاط الضعف المكتشفة.
استحداث عملية للتحقق من إصلاح الثغرات التي تتحقق بسرعة وفعالية من معالجة الثغرات عبر جميع فئات الأصول داخل البيئة.
ضمان معالجة الثغرات بفعالية من خلال أنشطة المعالجة القوية وإدارة التصحيح لتقليل مخاطر استغلال نقاط الضعف (إجراء المعالجة في الوقت المناسب ووفقَ أفضل ممارسة في الصناعة).
المقارنة بانتظام بين نتائج عمليات المسح المتتالية لنقاط الضعف، وذلك للتحقُّق من أنَّ نقاط الضعف قد تم علاجها في الوقت المناسب.

بالنسبة إلى خدمات المورّد المتعلقة باستضافة البنية التحتية/التطبيقات نيابة عن بنك باركليز،

يجب على المورّد إخطار بنك باركليز على الفور إذا تم تحديد أي نقاط ضعف حرجة/عالية.
تجب على المورّد معالجة نقاط الضعف بما يتماشى مع الجدول أدناه أو بالاتفاق مع بنك باركليز (مكتب الأمن الرئيس - فريق ECAM).

<table>
<tr><th>الأولوية</th><th>التصنيف</th><th>أيام الغلق (الحد الأقصى)</th></tr>
<tr><td>P1</td><td>حرج</td><td>15</td></tr>
<tr><td>P2</td><td>عالٍ</td><td>30</td></tr>
<tr><td>P3</td><td>متوسط</td><td>60</td></tr>
</table>
</td>
<td>إذا لم يتم تنفيذ هذا الضابط، فسيستطيع المهاجمون استغلال نقاط الضعف الكامنة في الأنظمة لتنفيذ هجمات سيبرانية، ما قد يؤدي إلى ضرر تنظيمي وإضرار بالسمعة.</td>
</tr>
</table>

	يجب إبلاغ/إخطار بنك باركليز فورًا بجميع المشكلات والثغرات الأمنية التي قد يكون لها تأثير مادي في البنية التحتية/تطبيقات الويب المقدمة من المورّد والتي يستضيفها بنك باركليز، التي قرر المورّد قبول المخاطرة بها، ومن ثم الحصول على موافقة بنك باركليز عليها كتابيًا (مكتب الأمن الرئيس - فريق ECAM). P4 | منخفض | 180 P5 | معلوماتي | 360	
22. إدارة التصحيح	يجب على المورّد وضع سياسات وإجراءات، وتطبيق عمليات تجارية/تدابير تنظيمية داعمة، وتنفيذ تدابير تقنية، وذلك لمراقبة/تتبع الحاجة إلى التصحيح ونشر تصحيحات الأمان لإدارة بيئة/ممتلكات المورّد بالكامل. يجب على المورّد التأكُّد من تطبيق أحدث التصحيحات الأمنية على الأنظمة/الأصول/الشبكات/التطبيقات في الوقت المناسب، ووفقَ أفضل ممارسة في الصناعة، مع ضمان ما يأتي: • ينبغي للمورّد اختبار جميع التصحيحات على الأنظمة التي تمثل بدقة تكوين أنظمة الإنتاج المستهدفة قبل نشر التصحيح على أنظمة الإنتاج وأن يتم التحقق من التشغيل الصحيح للخدمة المصححة بعد أي نشاط للتصحيح. إذا تعذر تصحيح النظام، فقم بنشر التدابير المضادة المناسبة. • يلزم تسجيل كل تغييرات تكنولوجيا المعلومات الرئيسة قبل التنفيذ واختبارها والموافقة عليها من خلال عملية إدارة تغيير قوية ومعتمدة لمنع أي انقطاع في الخدمة أو انتهاكات أمنية. • يجب على المورّد التأكُّد من انعكاس التصحيحات على بيئتَي الإنتاج والتعافي من الكوارث.	إذا لم يتم تنفيذ هذا الضابط، فقد تكون الخدمات عرضة لمشكلات الأمن التي قد تعرض بيانات المستهلك للخطر أو تسبب ضياع الخدمة أو تمكين نشاط ضار آخر.
23. محاكاة التهديد/اختبار الاختراق/تقييم أمن تكنولوجيا المعلومات	يتعين على المورد التعامل مع مزود أمن مؤهل ومستقل لإجراء تقييم لأمن تكنولوجيا المعلومات/محاكاة للتهديدات بما يشمل البنية التحتية لتكنولوجيا المعلومات ومن بينها موقع التعافي من الكوارث وتطبيقات الويب المتعلقة بالخدمة (الخدمات) التي يوفرها المورد لبنك باركليز. يجب القيام بذلك سنويًا على الأقل لتحديد الثغرات التي يمكن استغلالها لانتهاك سرية بيانات بنك باركليز من خلال الهجمات السيبرانية. كما يجب تحديد أولويات كل نقاط الضعف وتعقبها من أجل المعالجة. يجب تنفيذ الاختبار بما يتوافق مع أفضل ممارسة في الصناعة. بالنسبة إلى خدمات المورّد المتعلقة **باستضافة البنية التحتية/التطبيقات** نيابة عن بنك باركليز، • يلتزم المورد بإبلاغ بنك باركليز بنطاق التقييم الأمني والاتفاق معه عليه، وخصوصًا تاريخ/أوقات البدء والانتهاء، لمنع تعطيل أنشطة بنك باركليز الرئيسة. • يلزم إبلاغ بنك باركليز (مكتب الأمن الرئيس - فريق ECAM) بأي قضايا يتم قبولها والموافقة عليها، أو بكل تلك القضايا. • **تنبغي للمورّد مشاركة أحدث تقرير يتعلق بتقييم الأمن على أساس سنوي مع بنك باركليز (مكتب الأمن الرئيس - فريق ECAM)** • يجب على المورّد إخطار بنك باركليز على الفور إذا تم تحديد أي نقاط ضعف حرجة/عالية.	إذا لم يتم تنفيذ هذا الضابط، فقد لا يتمكن المورّدون من تقييم التهديدات السيبرانية التي يواجهونها والوقوف على مدى ملاءمة دفاعاتهم وقوتها على التصدي لها. قد يتم الكشف عن معلومات بنك باركليز و/أو قد يحدث فقدان للخدمة يسفر عن ضرر تنظيمي أو إضرار بالسمعة.

	• تجب على المورّد معالجة نقاط الضعف بما يتماشى مع الجدول أدناه أو بالاتفاق مع بنك باركليز (مكتب الأمن الرئيس - فريق ECAM). **الأولوية** / **التصنيف** / **أيام الغلق (الحد الأقصى)** P1 / حرج / 15 P2 / عالٍ / 30 P3 / متوسط / 60 P4 / منخفض / 180 P5 / معلوماتي / 360	
24. التشفير	• الأسباب المنطقية للتشفير - يتعين على المورد توثيق السبب المنطقي لاستخدام تكنولوجيا التشفير ومراجعة ذلك المبرر للتأكد من أنه لا يزال مناسبًا للغرض. • إجراءات دورة حياة التشفير - يتعين على المورد الاحتفاظ بمجموعة موثقة من إجراءات إدارة دورة حياة التشفير التي توضح بالتفصيل عمليات الشاملة لإدارة المفاتيح بدءًا من الإنشاء والتحميل والتوزيع وحتى الإتلاف. • الموافقة على العمليات اليدوية - يجب على المورّد التأكُّد من الحصول على اعتماد مناسب للأحداث التي يديرها العنصر البشري فيما يتعلق بالمفاتيح والشهادات الرقمية، ومن بينها التسجيل وإنشاء مفاتيح وشهادات جديدة، ومن الاحتفاظ بسجل للاعتماد. • الشهادات الرقمية - يجب على المورّد التأكُّد من اقتناء جميع الشهادات من مجموعة هيئات الشهادات (CA) المعتمدة والمدقَّقة التي توفر خدمات الإلغاء وسياسات إدارة الشهادات، كما يلزمه ضمان عدم استخدام الشهادات الموقعة ذاتيًا إلا في حال تعذر دعم حل مستند إلى هيئة للشهادات من الناحية الفنية، وأن تكون لديه ضوابط يدوية مطبقة لضمان سلامة المفاتيح وموثوقيتها وتحقيق الإلغاء والتجديد في الوقت المناسب. • إنشاء المفاتيح وفترة التشفير - يجب على المورّد التأكُّد من لزوم إنشاء كل المفاتيح بصورة عشوائية إما عن طريق أجهزة معتمدة أو من خلال مولد الأرقام العشوائية الزائفة الآمنة والمشفرة (CSPRNG) في البرنامج. o يجب على المورّد التأكُّد من أنَّ جميع المفاتيح تخضع بعد ذلك لدورة حياة تشفير محدودة ومحدَّدة بالوقت الذي يتم فيه استبدالها أو إلغاء تنشيطها. يجب أن يتوافق هذا أيضًا مع المعهد الوطني للمعايير والتكنولوجيا (NIST) وأفضل ممارسة في الصناعة. • حماية تخزين المفاتيح - يجب على المورّد التأكُّد من تقييد وجود المفاتيح المشفَّرة السرية/الخاصة بالأشكال الآتية: o في حدود التشفير لجهاز صلب/وحدة أمن صلبة معتمدة. o في شكل مشفر بموجب مفتاح قائم آخر أو مشتق من كلمة المرور. o في أجزاء مكونات منقسمة، ومقسمة بين مجموعات حفظ منفصلة. o المسح في ذاكرة المضيف طوال فترة عملية التشفير، ما لم تكن مطلوبة في حماية وحدة أمن الأجهزة (HSM).	تضمن حماية التشفير وخوارزمياته المحدَّثة والمناسبة حماية مستمرة لأصول معلومات بنك باركليز.

	• يجب على المورّد التأكّد من إنشاء المفاتيح والاحتفاظ بها داخل حدود ذاكرة وحدات HSM بالنسبة إلى المفاتيح عالية الأخطار. وهذا يتضمن: ○ مفاتيح الخدمات المنظمة التي يتم فيها تفويض وحدات HSM. ○ شهادات تمثل بنك باركليز من هيئات الشهادات (CA) العامة. ○ الشهادات الجذرية وشهادات الإصدار وبروتوكول أوضاع الشهادات على الإنترنت (OCSP) وهيئة التسجيل (RA) المستخدمة لإصدار الشهادات التي تحمي خدمات بنك باركليز. ○ المفاتيح التي تحمي المستودعات المجمَّعة والمخزَّنة الخاصة بالمفاتيح أو بيانات اعتماد المصادقة أو بيانات المعلومات المحددة للهوية الشخصية (PII). • النسخ الاحتياطي للمفاتيح وتخزينها - يحتفظ المورّد بنسخة احتياطية لكل المفاتيح لمنع انقطاع الخدمة في حالة تلف المفاتيح أو الحاجة إلى الاستعادة. يتم تقييد الوصول إلى النسخ الاحتياطية لتأمين المواقع الخاضعة لتقسيم المعرفة والتحكم المزدوج. يجب إخضاع النُّسخ الاحتياطية للمفاتيح لحماية تشفير لا تقل قوتها عن المفاتيح المستخدمة على الأقل. • الجرد - يحتفظ المورّد بجرد كامل ومُحدَّث لاستخدام التشفير في الخدمات التي يقدمها إلى بنك باركليز، بحيث يسرد تفاصيل كافة مفاتيح التشفير والشهادات الرقمية وبرامج التشفير وأجهزة التشفير التي يديرها المورّد لمنع التضرر في حال وقوع أي حادث. ويتم إثبات ذلك من خلال التوقيع على مراجعة الجرد على أساس ربع سنوي على الأقل ومن ثم تقديمها إلى بنك باركليز. يلزم أن تشمل قوائم الجرد ما يأتي عند الاقتضاء: ○ فريق دعم تكنولوجيا المعلومات ○ الأصول ذات الصلة ○ الخوارزميات وطول المفتاح والبيئة والتسلسل الهرمي للمفاتيح وهيئة الشهادات وبصمة الإصبع وحملية تخزين المفاتيح والغرض التقني والتشغيلي. • الغرض الوظيفي والتشغيلي - يجب أن يكون للمفاتيح غرض وظيفي وتشغيلي فردي ولا تتم مشاركتها بين خدمات متعددة أو خارج خدمات بنك باركليز. • مسارات التدقيق - يجب على المورّد إجراء مراجعة للسجلات القابلة للتدقيق ويحتفظ بدليل عليها على أساس ربع سنوي كحد أدنى، وذلك بالنسبة إلى جميع أحداث إدارة دورة حياة المفاتيح والشهادات التي توضح سلسلة العهدة الكاملة لجميع المفاتيح ومن بينها الإنشاء والتوزيع والتحميل والإتلاف، للكشف عن أي استخدام غير مصرح به. • الأجهزة - يُخزّن المورّد الأجهزة الصلبة في مناطق آمنة ويحتفظ بمسار للتدقيق طوال دورة حياة المفاتيح لضمان عدم المساس بسلسلة عهدة أجهزة التشفير. تُجرى مراجعة هذا المسار على أساس ربع سنوي. ○ يجب على المورّد التأكُّد من أنَّ جهاز التشفير معتمد وفق المستوى الثاني للمعيار FIPS140-2 على الأقل مع تحقيق المستوى 3 في الأمن المادي وإدارة مفاتيح التشفير أو معيار وحدة أمن أجهزة صناعة بطاقات السداد (PCI HSM). قد يختار المورّد السماح للبطاقات الذكية القائمة على الرقاقة أو الرموز الإلكترونية المعتمدة وفق معايير معالجة المعلومات الفيدرالية (FIPS) كأجهزة مقبولة لتخزين المفاتيح التي يمثلها الأفراد أو الزبائن ويحتفظون بها حال الوجود خارج الموقع. • اختراق المفاتيح - يحتفظ المورّد بخطة لاختراق المفاتيح ويراقبها لضمان إنشاء المفاتيح البديلة بمنأى عن المفتاح المخترق لمنع المفتاح المخترق من تقديم أي معلومات بخصوص بديله. في حال وقوع حادث اختراق، يلزم إخطار بنك باركليز عبر **مركز العمليات المشتركة (JOC) بمكتب الأمن الرئيس (CSO) ببنك باركليز** gcsojoc@barclays.com	

	• قوة الخوارزميات والمفاتيح - يضمن المورِّد توافق الخوارزميات وطول المفاتيح المستخدمة مع المعهد الوطني للمعايير والتكنولوجيا (NIST) وأفضل ممارسة في الصناعة.	
25. الحوسبة السحابية	يجب على المورِّد التأكُّد من ضرورة وجود إطار عمل محدَّد جيدًا للضوابط الأمنية في خدمة السحابة المستخدمة للخدمة (الخدمات) المقدَّمة إلى بنك باركليز، وذلك لحماية المفاهيم الأساسية للسريَّة والنزاهة والتوافر ولضمان وجود الضوابط الأمنية وعملها بفاعلية لحماية الخدمة (الخدمات) المقدَّمة إلى بنك باركليز. ينبغي اعتماد المورِّد وفقَ معيار ISO/IEC 27017 أو 27001 أو SOC 2 أو إطار عمل للأمان السحابي المماثل أو أفضل ممارسة في الصناعة للحصول على إجراءات ثابتة وأمنية مطبَّقة لضمان تأمين جميع استخدامات التكنولوجيا السحابية. تأكَّد من اعتماد موفِّر خدمة السحابة وفقَ أفضل ممارسة في الصناعة، بما في ذلك الضوابط المناسبة المكافئة لأحدث إصدار من تحالف أمان السحابة في مصفوفة ضوابط السحابة. تقع على عاتق المورِّد مسؤولية التأكُّد من أنَّ الضوابط الأمنية للبيانات المتعلقة بأصول معلومات/بيانات بنك باركليز، بما في ذلك البيانات الشخصية داخل السحابة وموفِّر خدمة السحابة، مسؤولة عن أمان خدمة السحابة. يظل المورِّد مسؤولاً عن تكوين تنفيذ الضوابط الأمنية ومراقبته للحماية من أي حوادث أمنية، بما في ذلك انتهاكات البيانات. يجب على المورِّد تنفيذ التدابير الأمنية عبر جميع جوانب الخدمة المُقدَّمة، بما في ذلك نموذج المسؤولية المشتركة في السحابة؛ بحيث يحافظ على السريَّة والنزاهة والتوافر وإمكانية الوصول عن طريق تقليل فرصة الأفراد غير المصرَّح لهم في الوصول إلى معلومات بنك باركليز والخدمات التي يستفيد منها بنك باركليز. ينبغي أن تغطي الضوابط الأمنية في السحابة، على سبيل المثال لا الحصر، مجالات نماذج النشر الآتية (البنية التحتية كخدمة (IaaS)/المنصة كخدمة (PaaS)/البرامج كخدمة (SaaS)): • آليات الحوكمة والمساءلة • إدارة الهوية والوصول • أمان الشبكة (بما في ذلك الاتصال) • أمان البيانات (العبور/عدم النشاط/التخزين) • التشفير والترميز وإدارة المفتاح - CEK • التسجيل والمراقبة • الوضع الظاهري • الفصل بين الخدمات تجب موافقة بنك باركليز (مكتب الأمن الرئيس - فريق ECAM) على أصول معلومات/بيانات بنك باركليز، بما في ذلك البيانات الشخصية المُخزَّنة في السحابة كجزء من الخدمة المُقدَّمة إلى بنك باركليز. عند الاحتفاظ بالبيانات الحسَّاسة (الشخصية والمقيِّدة) مع موفِّر خدمة السحابة، يجب على المورِّد تزويد بنك باركليز بالمواقع ومناطق البيانات ومناطق بيانات تجاوز الفشل حيث سيتم الاحتفاظ بهذه البيانات.	إذا لم يتم تنفيذ هذا الضابط الخاص بالسحابة، فقد تكون بيانات بنك باركليز عرضة للخطر، ما قد يؤدي إلى ضرر تنظيمي أو إضرار بالسمعة.
26. المساحة المخصصة للبنك (BDS)	بالنسبة إلى الخدمات المقدمة التي تتطلب مساحة رسمية مخصصة للبنك ((BDS، يلزم تطبيق متطلبات مادية وتقنية خاصة بمساحة BDS. (إذا كانت مساحة BDS تمثل أحد متطلبات الخدمة، فستكون متطلبات الضابط منطبقة).	إذا لم يتم تنفيذ هذا الضابط، فقد لا يتم وضع الضوابط المادية والتقنية المناسبة، ما يؤدي إلى

	تتمثل أنواع مساحة BDS المختلفة الأخرى في: المستوى 1 (الدرجة الأولى) - تتم إدارة البنية التحتية لتكنولوجيا المعلومات بالكامل من قِبل **بنك باركليز** من خلال توفير أجهزة LAN وWAN وسطح المكتب المدارة من **بنك باركليز** إلى موقع المورّد الذي يتضمن المساحة المخصصة لبنك باركليز. المستوى 2 (درجة الأعمال) - تتم إدارة البنية التحتية لتكنولوجيا المعلومات بالكامل بواسطة **المورِّد** وتتصل ببوابات الشبكة الخارجية **لبنك باركليز** - يمتلك المورّد أجهزة LAN وWAN وسطح المكتب ويديرها. المستوى 3 (الدرجة الاقتصادية) - تتم إدارة البنية التحتية لتكنولوجيا المعلومات بالكامل بواسطة **المورِّد** وتتصل ببوابات الإنترنت من **بنك باركليز** - يمتلك المورّد أجهزة LAN وWAN وسطح المكتب ويديرها.	تأخير الخدمة أو تعطيلها أو حدوث انتهاكات أمنية سيبرانية/حوادث أمنية.
26.1 المساحة المخصصة للبنك - الفصل المادي	يلزم أن تكون المساحة الفعلية المشغولة مخصصة لبنك باركليز ولا تتم مشاركتها مع غيرها من الشركات/البائعين. كما يلزم أن تكون منفصلة انفصالاً منطقيًا وماديًا.	
26.2 المساحة المخصصة للبنك - التحكم في الوصول المادي	• يلزم أن تكون لدى المورّد عملية وصول مادي تتناول طرق الوصول والتصريح به إلى مساحة BDS حيث يتم تقديم الخدمات. • يلزم تقييد الدخول إلى مساحة BDS والخروج منها ومراقبتها من خلال آليات التحكم في الوصول المادي لضمان عدم السماح لغير الموظفين المصرح لهم بالدخول. • بطاقة وصول إلكترونية مصرح بها للوصول إلى مساحات BDS في المنشأة. • يتعين على المورد إجراء فحوصات ربع سنوية لضمان عدم حصول غير الأفراد المصرح لهم على الوصول إلى مساحة BDS. تجرى دراسة الاستثناءات بدقة تامة. • تتم إزالة حقوق الوصول في غضون 24 ساعة بالنسبة إلى جميع المغادرين والمنتقلين (والسجلات المناسبة المطلوب الاحتفاظ بها). • استخدام الحراس للقيام بدوريات روتينية داخل مساحة BDS لتحديد الوصول غير المصرح به أو النشاط الضار المحتمل بفعالية • يلزم تنفيذ ضوابط التأمين التلقائية للوصول إلى مساحة BDS، وتشمل: ما إذا كان للموظفين المصرح لهم: ○ شارة هوية تحمل صورة مرئية طوال الوقت ○ يتم تطبيق قارئات البطاقات التي تعمل بالتقريب ○ يتم تمكين آلية المرور مرة واحدة فقط • يلزم أن يتبنى المورد عمليات وإجراءات للتحكم في الأشخاص الخارجيين ومراقبتهم، ومن بينهم الجهات الخارجية التي لديها إمكانية الوصول المادي إلى مساحات BDS لأغراض الصيانة وعمال النظافة.	
26.3 BDS - المراقبة بالفيديو	• تنفيذ مراقبة مساحة BDS بالفيديو للكشف الفعال عن الوصول غير المصرح به أو النشاط الضار والمساعدة في التحقيقات. • تلزم مراقبة جميع نقاط الدخول إلى مساحة BDS والخروج منها بالفيديو. • يتم وضع الكاميرات الأمنية بشكل مناسب وتوفر صورًا واضحة يمكن تحديدها طوال الوقت لالتقاط النشاط الضار والمساعدة في التحقيقات. يتعين على المورد تخزين لقطات الكاميرا التلفزيونية المغلقة (CCTV) التي يتم التقاطها لمدة 30 يومًا ويلزم تأمين مواقع جميع تسجيلات ومسجلات CCTV لمنع التعديل أو الحذف أو العرض "غير الرسمي" لأي شاشات CCTV مرتبطة ويلزم كذلك التحكم في الوصول إلى التسجيلات وحصره على الأفراد المصرح لهم فقط.	
26.4 BDS - الوصول إلى شبكة بنك باركليز ورموز مصادقة بنك باركليز	• يلتزم كل مستخدم فردي بالاكتفاء فقط بمصادقة الوصول إلى شبكة بنك باركليز من مساحة BDS باستخدام رمز المصادقة متعددة العوامل المقدم من بنك باركليز. • يجب على المورّد الاحتفاظ بسجلات للأفراد الذين يتم تزويدهم برموز مصادقة بنك باركليز كما يجب عليه إجراء تسوية على أساس ربع سنوي.	

	• سيلغي بنك باركليز تنشيط بيانات اعتماد المصادقة عند الإخطار بأنه لم تعد هناك حاجة إلى الوصول (كأن يتم إنهاء عمل الموظف، إعادة تعيين المشروع، إلخ) في غضون أربع وعشرين (24) ساعة. • سيقوم بنك باركليز بإلغاء تنشيط بيانات اعتماد المصادقة على الفور في حال عدم استخدامها لفترة من الوقت (لا تتجاوز فترة عدم الاستخدام هذه شهرًا واحدًا). • يلزم اعتماد الخدمات التي تتمتع بإمكانية الوصول إلى الطباعة عن بُعد عبر تطبيق Barclays Citrix وترخيصها من قِبل بنك باركليز (مكتب الأمن الرئيس - فريق ECAM). يجب على المورّد الاحتفاظ بالسجلات وإجراء التسوية على أساس ربع سنوي. الرجوع إلى المراقبة - 12 العمل عن بُعد (الوصول عن بُعد)
26.5 المساحة المخصصة للبنك - الدعم خارج المكتب	لا يتم توفير الوصول عن بعد إلى بيئة BDS بصورة افتراضية لدعم ساعات العمل خارج المكتب/خارج ساعات العمل/العمل من المنزل. تجب الموافقة على أي وصول عن بُعد من قِبل فرق بنك باركليز ذات الصلة (ومن بينها مكتب الأمن الرئيس - فريق ECAM).
26.6 المساحة المخصصة للبنك - أمن الشبكة	• الاحتفاظ بقائمة جرد محدَّثة لجميع حدود شبكة المؤسسة (من خلال بنية الشبكة/الرسم التخطيطي الخاص بها). • تلزم مراجعة تصميم الشبكة وتنفيذها على أساس سنوي على الأقل. • يجب الفصل المنطقي بين شبكة BDS وشبكة شركة المورّد باستخدام جدار الحماية، كما يلزم تقييد حركة المرور الواردة والصادرة ومراقبتها. • يجب أن يقتصر ضمان تكوين التوجيه على الاتصالات بشبكة بنك باركليز فقط كما يجب عدم القيام بالتوجيه إلى أي شبكات أخرى للمورّدين. • يجب إجراء تكوين آمن لموجه الحافة الخاص بالمورّد والمتصل ببوابات الشبكة الخارجية لبنك باركليز باستخدام مفهوم الحد من ضوابط المنافذ والبروتوكولات والخدمات؛ ○ التأكد من ضرورة تمكين التسجيل والمراقبة. • تلزم مراقبة شبكة BDS وتقييد السماح بالأجهزة المصرح لها فقط من خلال الضوابط المناسبة للوصول إلى الشبكة الرجوع إلى المراقبة - 10 أمن الحدود والشبكات
26.7 المساحة المخصصة للبنك – الشبكة اللاسلكية	يجب تعطيل الشبكات اللاسلكية لقطاع شبكة بنك باركليز لتوفير خدمات بنك باركليز.
26.8 المساحة المخصصة للبنك - أمن نقطة النهاية	يجب تكوين تصميمات سطح مكتب آمنة وفقَ أفضل ممارسة في الصناعة لأجهزة الكمبيوتر داخل شبكة BDS. لا بد من وضع أفضل الممارسات في الصناعة في مكانها، كما يجب أن يتضمن إنشاء أمان أجهزة نقاط نهاية BDS، على سبيل المثال لا الحصر، ما يأتي: • تشفير الأقراص؛ • تعطيل جميع البرامج/الخدمات/المنافذ غير المطلوبة؛ • تعطيل الوصول إلى حقوق الإدارة للمستخدم المحلي، • لن يتم السماح لموظفي المورّد بتغيير الإعدادات الأساسية مثل: حزمة الخدمة الافتراضية والخدمات الافتراضية وما إلى ذلك، • يجب تعطيل منفذ USB لمنع نسخ بيانات بنك باركليز إلى الوسائط الخارجية؛ • التحديث باستخدام أحدث توقيعات مكافحة الفيروسات وتصحيحات الأمان، • تقييد منع فقدان البيانات بعدم استخدام القص والنسخ واللصق وطباعة الشاشة أو أداة الالتقاط مع بيانات بنك باركليز، • يجب تعطيل الوصول إلى الطابعة، بصورة افتراضية؛ • ينبغي تعطيل مشاركة/نقل أصول معلومات/بيانات بنك باركليز باستخدام أدوات/برامج المراسلة الفورية؛

	• توافر القدرة والعمليات الخاصة باكتشاف البرامج غير المصرح بها والتي يتم تحديدها بوصفها ضارة ومنع تثبيت البرامج غير المصرح بها؛ الرجوع إلى المراقبة - 16 أمن نقطة النهاية	
26.9 المساحة المخصصة للبنك - البريد الإلكتروني والإنترنت	• يلزم تكوين اتصال الشبكة بأمان لتقييد نشاط البريد الإلكتروني والإنترنت على شبكة BDS. • يلتزم المورد بتقييد القدرة على الوصول إلى مواقع الشبكات الاجتماعية وخدمات بريد الويب والمواقع بإمكانية تخزين المعلومات على الإنترنت كاستخدام google drive وDropbox وiCloud. • تلزم حماية النقل غير المصرح به لبيانات بنك باركليز خارج شبكة BDS من تسرب البيانات: • البريد الإلكتروني • بوابة الإنترنت/الويب (بما في ذلك التخزين عبر الإنترنت والبريد الإلكتروني) • تطبيق عوامل تصفية عناوين URL المستندة إلى الشبكة والتي تقيد قدرة النظام بالاتصال فقط بمواقع الويب الداخلية أو مواقع الإنترنت الخاصة بمؤسسة المورّد • حظر كل المرفقات و/أو ميزة التحميل إلى مواقع الويب. • التأكد من تقييد السماح بمتصفحات الويب وعملاء البريد الإلكتروني المدعومة بالكامل فقط.	
26.10 BDS - BYOD/الجهاز الشخصي	**يلزم عدم السماح للأجهزة الشخصية/BYOD بالوصول إلى بيئة بنك باركليز و/أو بياناته**	
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 المتعاقدون معه من الباطن لاستحداث أنظمة المورد المستخدمة في الخدمات أو اختبارها أو تعزيزها أو صيانتها أو تشغيلها، من أجل مراجعة امتثال المورد لالتزاماته. يجب على المورّد أيضًا السماح لبنك باركليز بإجراء الفحص على أساس سنوي على الأقل أو فور وقوع حادث أمني. يلزم إجراء تقييم المخاطر من جانب بنك باركليز فيما يتعلق بأي عدم امتثال للضوابط التي يحددها بنك باركليز في أثناء التفتيش كما يجب أن يحدد بنك باركليز إطارًا زمنيًا للتصحيح. يتعين على المورد بعد ذلك إكمال أي إصلاح مطلوب خلال هذا الإطار الزمني. يلتزم المورد بتقديم كل الدعم المطلوب بصورة معقولة من قِبل بنك باركليز فيما يتعلق بأي فحص، كما يلزم استكمال التوثيق المقدَّم في أثناء التفتيش ومن ثم إعادته إلى بنك باركليز.	إذا لم يتم الاتفاق، فلن يتمكن الموردون من تقديم ضمان كامل للامتثال لهذه الالتزامات الأمنية.

الملحق A: مسرد المصطلحات

	التعريفات
الحساب	مجموعة بيانات اعتماد (كمعرف المستخدم وكلمة المرور) تتم من خلالها إدارة الوصول إلى نظام تكنولوجيا المعلومات باستخدام ضوابط الوصول المنطقي.
النسخ الاحتياطي	يشير النسخ الاحتياطي أو عملية النسخ الاحتياطي إلى عمل نُسخ من البيانات بحيث يمكن استخدام هذه النُسخ الإضافية لاستعادة الأصل بعد حدث ضياع البيانات.
المساحة المخصصة للبنك	تشير المساحة المخصصة للبنك (BDS) إلى أي منشأة في حوزة أحد أعضاء مجموعة الموردين أو أي متعاقد من الباطن أو تقع تحت سيطرته وتكون مخصصة حصريًا لبنك باركليز ويتم تنفيذ الخدمات أو تسليمها منها.
أفضل ممارسة في الصناعة	استخدام أفضل الممارسات والعمليات والمعايير والشهادات الرائدة الحالية في السوق؛ وممارسة تلك الدرجة من المهارة والرعاية التي يمكن توقعها بشكل معقول من مؤسسة مهنية ذات مهارات عالية وخبرة ورائدة في السوق تشارك في تقديم خدمات مماثلة أو مشابهة للخدمات المُقدَّمة إلى باركليز.
BYOD	جلب الجهاز الشخصي
التشفير	تطبيق النظرية الرياضية لتطوير التقنيات والخوارزميات التي يمكن تطبيقها على البيانات لضمان تحقيق أهداف مثل السرية و/أو سلامة البيانات و/أو التوثيق.
الأمن السيبراني	تطبيق التقنيات والعمليات والضوابط والتدابير التنظيمية لحماية أنظمة الكمبيوتر والشبكات والبرامج والأجهزة والبيانات من الهجمات الرقمية التي قد تشمل (على سبيل المثال لا الحصر)، الكشف غير المصرَّح به عن الأجهزة أو البرامج أو البيانات، أو تدميرها أو فقدانها أو تعديلها أو سرقتها أو تلفها.
البيانات	تسجيل للحقائق أو المفاهيم أو التعليمات على وسيط تخزين للنقل والاسترجاع والمعالجة باستخدام الوسائل الآلية والعرض التقديمي في صورة معلومات يمكن للعنصر البشري استيعابها.
حجب الخدمة (هجوم)	محاولة لحجب توافر أحد موارد الكمبيوتر لمستخدميه المعنيين.
الإتلاف/الحذف	إجراء استبدال المعلومات أو محوها أو إتلافها ماديًا بحيث لا يمكن استعادتها.
ECAM	فريق ضمان ومراقبة الشبكات السيبرانية الخارجية الذي يقيّم الوضع الأمني لدى المورّد
التشفير	تحويل الرسالة (بيانات أو صوت أو فيديو) إلى شكل لا معنى له ولا يمكن للقراء غير المصرح لهم فهمه. ويتم هذا التحويل من تنسيق النص العادي إلى تنسيق النص المشفر.
HSM	وحدة أمن الأجهزة. جهاز مخصص يوفر إنشاء مفتاح تشفير آمن وتخزينه واستخدامه، متضمنًا تسريع عمليات التشفير.
أصول المعلومات	أي معلومات قيّمة، يتم النظر فيها من حيث متطلبات السرية والسلامة والتوافر. أو أي معلومة منفردة أو مجموعة معلومات ذات قيمة بالنسبة إلى المؤسسة.
مالك أصول المعلومات	فرد داخل المؤسسة يكون مسؤولاً عن تصنيف الأصل وضمان التعامل معه بطريقة صحيحة وملائمة.
أقل امتياز	أدنى مستوى للوصول/للأذونات يمكّن المستخدم أو الحساب من أداء دوره التجاري.
جهاز الشبكة/تجهيزات الشبكات	أي جهاز تكنولوجيا معلومات متصل بشبكة يتم استخدامه لإدارة الشبكة أو دعمها أو التحكم فيها. ويمكن أن يشمل، على سبيل المثال لا الحصر، أجهزة التوجيه والمحولات وجدران الحماية وموزّع الأحمال.
التعليمة البرمجية الضارة	برنامج مكتوب بقصد التحايل على السياسة الأمنية لنظام أو جهاز أو تطبيق خاص بتكنولوجيا المعلومات. تشمل الأمثلة فيروسات الكمبيوتر وأحصنة طروادة والفيروسات المتنقلة.
المصادقة متعددة العوامل	مصادقة تتطلب زوجًا أو أكثر من تقنيات المصادقة المختلفة. يتمثل أحد الأمثلة في استخدام رمز الأمان، حيث تعتمد المصادقة الناجحة على شيء يحمله الفرد (مثل رمز الأمان) وشيء يعرفه المستخدم (أي رمز PIN الخاص برمز الأمان).
البيانات الشخصية	أي معلومات تتعلق بشخص طبيعي محدَّد الهوية أو يمكن تحديد هويته ("صاحب البيانات")؛ الشخص الطبيعي الذي يمكن تحديد هويته هو شخص 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.
الوصول المميز	تعيين وصول خاص (فوق القياسي) أو أذونات أو قدرات لمستخدم أو عملية أو جهاز كمبيوتر.

الحساب المميز	حساب يوفر مستوى مرتفعًا 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, تشمل الأمثلة: حسابات "المسؤول" و"الأصلي" ويونكس ذات معرّف فريد = 0، وحسابات الدعم وحسابات إدارة الأمن وحسابات إدارة النظام وحسابات المسؤول المحلي
الوصول عن بعد	التكنولوجيا والتقنيات المستخدمة لمنح المستخدمين المصرح لهم وصولاً إلى شبكات المؤسسة وأنظمتها من موقع خارج الموقع.
النظام	يشير النظام، في سياق هذا المستند، إلى العنصر البشري والإجراءات وتجهيزات تكنولوجيا المعلومات والبرمجيات. تُستخدم عناصر هذا الكيان المركب معًا في بيئة التشغيل أو الدعم المستهدفة لأداء مهمة معينة أو تحقيق غرض معين أو تقديم دعم أو تحقيق مطلب.
ينبغي	يعني هذا التعريف أنَّ الآثار المترتبة سيتم استيعابها تمامًا وتقييمها بعناية.
حادث أمني	تُعرَّف الحوادث الأمنية على أنها تلك الأحداث التي تتضمن، على سبيل المثال لا الحصر، ما يأتي: • محاولات (سواء أكانت فاشلة أم ناجحة) للوصول غير المصرح به إلى نظام معين أو بياناته. • انقطاع الخدمة أو رفضها على نحو غير مرغوب فيه. • استخدام غير مصرح به لنظام معالجة البيانات أو تخزينها. • تغييرات في خصائص أجهزة النظام أو البرامج الثابتة أو البرامج دون معرفة المالك أو توجهات منه أو موافقته. • ثغرة في التطبيق تؤدي إلى وصول غير مصرح به إلى البيانات.

الملحق B: مخطط التسميات المعلوماتية لبنك باركليز

الجدول B1: 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). 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 • معلومات التخطيط الإستراتيجي - التجارية والتنظيمية • معلومات محددة حول تهيئة نظام المعلومات • نتائج تدقيق وتقارير محددة • محاضر اللجنة التنفيذية • تفاصيل المصادقة أو التعريف والتحقُّق (ID&V) - الزبون/العميل والزميل • كميات كبيرة من معلومات حامل البطاقة • توقعات الأرباح أو النتائج المالية السنوية (قبل نشرها للجمهور) • 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. وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي). ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة.	• الإستراتيجيات والميزانيات • تقييم الأداء • رواتب الموظفين وبياناتهم الشخصية • 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. وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي). ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة.	• خطط منتجات جديدة • عقود العملاء • العقود القانونية • معلومات الأفراد/معلومات زبائن/عملاء الأحجام المنخفضة المقرر إرسالها خارجيًا • معلومات الزبائن/العملاء. • مواد عرض الإصدار الجديد (مثل نشرة الإصدار، مذكرة العرض) • مستندات البحث النهائية • المعلومات الجوهرية غير العامة وغير التابعة لبنك باركليز (MNPI) • كل التقارير البحثية • المواد التسويقية المحددة • تعليقات السوق • 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 • المنشورات • الإعلانات العامة • إعلانات الوظائف

		• المعلومات التي لا تأثير لها في بنك باركليز

الجدول B2: مخطط التسميات المعلوماتية لبنك باركليز - متطلبات المعالجة

*** 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	• يلزم تعيين مالك لأصول المعلومات للأصول.	• يلزم تعيين مالك لأصول المعلومات للأصول.	• يلزم تعيين مالك لأصول المعلومات للأصول.
التخزين	• 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 مخولين عليها. • 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). • 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. • 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). • يتعين طباعة الأصول من خلال استخدام أدوات طباعة آمنة. • 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. • يلزم عدم ترك الأصول (سواء أكانت مادية أم إلكترونية) في مواقع عامة داخل المنشآت والتي قد يكون للزوار فيها وصول غير خاضع للإشراف. • 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). • يلزم استرداد الأصول المطبوعة على الفور من الطابعة. وفي حال عدم التمكن من ذلك، يلزم الاستعانة بأدوات الطباعة الآمنة. • تلزم حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة.
المشاركة	• يتعين إرفاق ملصق معلوماتي واضح على كل صفحة من صفحات الأصول المطبوعة. • 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. • 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. • يتعين أن تحتوي الأصول الإلكترونية على ملصق معلوماتي واضح. • 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 معلوماتي واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين إرفاق ملصق معلوماتي واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة • 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 يقتصر توزيع الأصول على النظم أو الأساليب أو الموردين المعتمدين من قبل المؤسسة.

	• 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 أصول 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.		• 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.
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 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. • 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.

السرية البنكية

ضوابط إضافية حصرية فقط لدوائر الاختصاص القضائي للسرية البنكية (سويسرا/موناكو)

مجال/عنوان الرقابة	وصف الرقابة	الأهمية
1. الأدوار والمسؤوليات	يجب على المورّد تحديد الأدوار والمسؤوليات والمساءلات ومشاركتها فيما يتعلق بالتعامل مع البيانات المحدّدة لهوية العميل (يشار إليها فيما يأتي بالاختصار CID). تجب على المورّد مراجعة الوثائق التي تسلّط الضوء على الأدوار والمسؤوليات والمساءلات الخاصة بالبيانات المحدّدة لهوية العميل بعد أي تغيير جوهري في نموذج تشغيل المورّد (أو الأعمال) أو مرة واحدة على الأقل سنويًا، ومن ثم توزيعها مع دوائر اختصاص السرية البنكية المناسبة. يجب أن تشمل الأدوار الرئيسة مسؤولاً تنفيذيًا كبيرًا، يتحمل مسؤولية حماية جميع الأنشطة المتعلقة بالبيانات المحدّدة لهوية العميل والإشراف عليها (يرجى الرجوع إلى الملحق A لتعريف CID). يلزم أن يبقى عدد الموظفين الذين يمكنهم الوصول إلى بيانات CID عند الحد الأدنى، بناءً على مبدأ الحاجة إلى المعرفة.	يدعم التحديد الواضح للأدوار والمسؤوليات تنفيذ جدول التزامات الرقابة على الموردين الخارجيين.
2. الإبلاغ عن انتهاك بيانات CID	لا بد من وجود ضوابط وعمليات وإجراءات موثَّقة في مكانها لضمان الإبلاغ عن أي انتهاكات تؤثر في البيانات المحدّدة لهوية العميل وإدارتها. لا بد من الاستجابة لأي انتهاك لمتطلبات المعالجة (على النحو المحدَّد في الجدول B2) من قِبل المورّد ومن ثم إبلاغ كيان بنك باركليز المطابق والمعني بالسرية البنكية على الفور (في غضون 24 ساعة على أبعد تقدير). لا بد من إنشاء عملية استجابة للحوادث للتعامل في الوقت المناسب مع الأحداث التي تنطوي على البيانات المحدّدة لهوية العميل والإبلاغ المنتظم عنها، واختبارها بانتظام. يجب على المورّد ضمان اتباع الإجراءات التصحيحية المطبقة بعد وقوع حادث من خلال وضع خطة تصحيح (الإجراء والملكية وتاريخ التنفيذ) ومشاركتها مع دائرة اختصاص السرية البنكية المطابقة واعتمادها من قِبلها. ينبغي للمورّد اتخاذ إجراء تصحيحي في الوقت المناسب. في حال قيام المورّد الخارجي بتقديم خدمات استشارية، وتسبب أحد موظفي هذا المورّد في وقوع حوادث منع فقدان البيانات، فسيقوم البنك بإخطار المورّد بالحادث وسيحق له، عند الاقتضاء، طلب استبدال الموظف.	تساعد عملية الاستجابة للحوادث على ضمان احتواء الحوادث بسرعة ومنع تصعيدها. قد يترتب على أي انتهاك يؤثر في بيانات CID إضرار قوي بالسمعة وإضرار ببنك باركليز ويمكن أن يؤدي إلى فرض غرامات وفقدان الترخيص البنكي في سويسرا أو موناكو
3. التثقيف والتوعية	يتعين على موظفي المورد الذين لديهم حق الوصول إلى بيانات CID و/أو يتعاملون معها استكمال تدريب* يتناول متطلبات السرية البنكية لبيانات CID، بعد أي تغيير في اللوائح أو بمعدل مرة واحدة سنويًا على الأقل. يتعين على المورد ضمان استكمال جميع موظفيه الجدد (الذين لديهم إمكانية الوصول إلى بيانات CID و/أو يتعاملون معها)، خلال فترة زمنية معقولة (حوالي 3 أشهر)، تدريبًا يضمن استيعابهم مسؤولياتهم فيما يتعلق ببيانات CID. يتعين على المورد تتبع موظفيه الذين يستكملون التدريب. * دوائر اختصاص السرية البنكية لتقديم إرشادات حول محتوى التدريب المتوقع.	يدعم التعليم والتثقيف كل الضوابط الأخرى ضمن هذا الجدول الزمني.

4. مخطط التسميات المعلوماتية	***عند الاقتضاء** *، يتعين على المورد تطبيق مخطط التسميات المعلوماتية لبنك باركليز (الجدول E1 من الملحق E، أو مخطط بديل متفق عليه مع دائرة اختصاص السرية البنكية، على جميع أصول المعلومات المحتفظ بها أو التي تتم معالجتها نيابة عن دائرة اختصاص السرية البنكية. تتوافر متطلبات معالجة بيانات CID في الجدول E2 من الملحق E. * يشير مصطلح **"عند الاقتضاء"** إلى *ميزة الموازنة بين التسميات والمخاطر المرتبطة. على سبيل المثال، تُعد تسمية مستند ما أمرًا غير مناسب، حال كان ذلك مخالفًا للمتطلبات التنظيمية لمكافحة التزوير والتلاعب.*	يعد الجرد الكامل والدقيق لأصول المعلومات ضروريًا لضمان الضوابط المناسبة.
5. الحوسبة السحابية/التخزين الخارجي	تجب الموافقة على جميع استخدامات الحوسبة السحابية و/أو التخزين الخارجي للبيانات المحدِّدة لهوية العميل (في الخوادم خارج نطاق دائرة اختصاص السرية البنكية أو خارج البنية التحتية للمورّد) المستخدمة كجزء من الخدمة المقدمة إلى دائرة الاختصاص هذه من قِبل الفرق المحلية ذات الصلة (ومن بينها مكتب الأمن الرئيس، الامتثال والقانون)، كما يجب تنفيذ الضوابط وفقَ القوانين واللوائح المعمول بها في دائرة اختصاص السريَّة البنكية المطابقة من أجل حماية معلومات البيانات المحدِّدة لهوية العميل فيما يتعلق بالملف عالي الأخطار الذي يقدمونه.	إذا لم يتم تنفيذ هذا المبدأ، فقد تكون بيانات العميل المحمية (البيانات المحدِّدة لهوية العميل) على نحو غير ملائم عرضة للخطر، ما قد يؤدي إلى فرض عقوبات قانونية وتنظيمية، أو إضرار بالسمعة.

الملحق C: مسرد المصطلحات

** تُعد البيانات المحدِّدة لهوية العميل بيانات خاصة بموجب قوانين السريَّة البنكية المعمول بها في سويسرا وموناكو. وعلى هذا النحو، فإن الضوابط المدرجة هنا مكملة لتلك المذكورة أعلاه.

المصطلح	التعريف
CID	البيانات المحدِّدة لهوية العميل
CIS	أمن المعلومات والأمن السيبراني
موظف المورد	أي فرد يعينه المورّد مباشرة كموظف دائم، أو أي فرد يقدّم خدمات إلى المورّد لفترة زمنية محدودة (كالاستشاري)
الأصل	أي معلومة منفردة أو مجموعة معلومات ذات قيمة بالنسبة إلى المؤسسة
النظام	يشير النظام، في سياق هذا المستند، إلى العنصر البشري والإجراءات وتجهيزات تكنولوجيا المعلومات والبرمجيات. تُستخدم عناصر هذا الكيان المركب معًا في بيئة التشغيل أو الدعم المستهدفة لأداء مهمة معينة أو تحقيق غرض معين أو تقديم دعم أو تحقيق مطلب.
المستخدم	حساب يتم تعيينه للموظف أو الاستشاري أو المتعاقد أو عامل الوكالة لدى المورد ممن لديهم تصريح بالوصول إلى نظام مملوك لبنك باركليز دون امتيازات تصاعدية.

الملحق D: تعريف البيانات المحددة لهوية العميل

بيانات CID المباشرة (DCID) يمكن تعريفها بوصفها المعرفات الفريدة (المملوكة للعميل) التي تسمح، بذاتها ومن تلقاء نفسها، بتحديد هوية العميل دون الوصول إلى البيانات الموجودة في تطبيقات بنك باركليز البنكية. يلزم أن تكون هذه البيانات واضحة، دون أن تخضع لتفسير، ويمكن أن تتضمن معلومات مثل الاسم الأول، واسم العائلة، واسم الشركة، والتوقيع، ومعرف الشبكة الاجتماعية وما إلى ذلك.

بيانات CID غير المباشرة (ICID) تنقسم إلى 3 مستويات

- L1 ICID يمكن تعريفها بوصفها معرفات فريدة (مملوكة للبنك) تسمح بتحديد هوية العميل بمفردها في الحالات التي يتم فيها توفير الوصول إلى التطبيقات البنكية أو **تطبيقات الجهات الخارجية** الأخرى. يلزم أن يكون المعرّف واضحًا دون أن يخضع لتفسير، ويمكن أن يتضمن معرّفات مثل رقم الحساب ورمز IBAN ورقم بطاقة الائتمان وما إلى ذلك.
- L2 ICID يمكن تعريفها بوصفها معلومات (مملوكة للعميل) توفر، بالاقتران مع غيرها من المعلومات الأخرى، استنتاجًا لهوية العميل. في حين أنه لا يمكن استخدام هذه المعلومات بمفردها لتحديد هوية العميل، فإنه يمكن استخدامها مع معلومات أخرى لتحديد هوية العميل. تلزم حماية بيانات L2 ICID وإدارتها بمستوى الصرامة نفسه الخاص ببيانات DCID.
- L3 ICID يمكن تعريفها بوصفها معرفات فريدة ولكنها مجهولة المصدر (مملوكة للبنك) وتسمح بتحديد هوية العميل إذا تم توفير الوصول إلى التطبيقات البنكية. ويتمثل الفرق بينها وبين بيانات L1 ICID في تصنيف المعلومات بوصفها مقيدة - خارجية بدلاً من سرية بنكية، ما يعني أنها لا تخضع للضوابط نفسها.

يرجى الرجوع إلى الشكل 1، تسلسل قرارات بيانات CID للحصول على نظرة عامة على أسلوب التصنيف.

يلزم عدم مشاركة بيانات L1 ICID المباشرة وغير المباشرة مع أي شخص موجود خارج البنك كما يلزم احترام مبدأ الحاجة إلى المعرفة طوال الوقت. يمكن مشاركة بيانات L2 ICID على أساس الحاجة إلى المعرفة، ولكن يتعين عدم مشاركتها بالاقتران مع أي جزء آخر من بيانات CID. فمن خلال مشاركة أجزاء متعددة من بيانات CID، تكون ثمة احتمالية إنشاء "تركيبة ضارة" يمكن أن تكشف عن هوية العميل. إننا نحدد التوليفة الضارة بكونها تبدأ بجزأين على الأقل من بيانات L2 ICID. تمكن مشاركة بيانات L3 ICID لأنها غير مصنفة كمعلومات على مستوى السرية البنكية، إلا إذا كان من المحتمل أن يترتب على الاستخدام المتكرر للمعرف نفسه جمع كمية من بيانات L2 ICID كافية للكشف عن هوية العميل.

تصنيف المعلومات	السرية البنكية			مقيَّدة - داخلية
التصنيف	بيانات CID المباشرة (DCID)	بيانات CID غير المباشرة (ICID)		
		غير المباشرة (المستوى 1)	غير المباشرة جزئيًا (المستوى 2)	معرّف غير شخصي (المستوى 3)
نوع المعلومات	اسم العميل	رقم الحاوية/معرف الحاوية	محل الميلاد	أي معرف داخلي صارم لتطبيق استضافة/معالجة بيانات CID
	اسم الشركة	رقم MACC (حساب نقدي تحت معرف حاوية أفالوك)	تاريخ الميلاد	المعرف الديناميكي
	كشف الحساب	معرف خدمات البيانات المشتركة (SDS)	الجنسية	معرف دور جهة إدارة علاقات العملاء (CRM)
	التوقيع	رمز IBAN	العنوان	معرف هوية الحاوية الخارجية
	معرف هوية الشبكة الاجتماعية	تفاصيل تسجيل الدخول إلى الخدمات البنكية الإلكترونية	الوضع العائلي	
	رقم جواز السفر	رقم الإيداع الآمن	الرمز البريدي	
	رقم الهاتف	رقم بطاقة الائتمان	حالة الثروة	
	عنوان البريد الإلكتروني	مراسلات SWIFT	حجم الصفقات/المعاملات الكبير	
	لقب وظيفي أو لقب شخصية سياسية بارزة (PEP)	المعرّف الداخلي لشريك العمل	آخر زيارة للعميل	
	اسم فنان		اللغة	
	عنوان IP		النوع	
	رقم الفاكس		تاريخ انتهاء بطاقة الائتمان	
			مسؤول الاتصال الرئيس	
			محل الميلاد	
			تاريخ فتح الحساب	

مثال: إذا أرسلت بريدًا إلكترونيًا أو شاركت أي مستند مع أشخاص خارجيين (ومن بينهم جهات خارجية في سويسرا/موناكو) أو زملاء داخليين في شركة تابعة/شركة فرعية أخرى موجودة في سويسرا/موناكو أو دول أخرى (مثل المملكة المتحدة)

1. اسم العميل

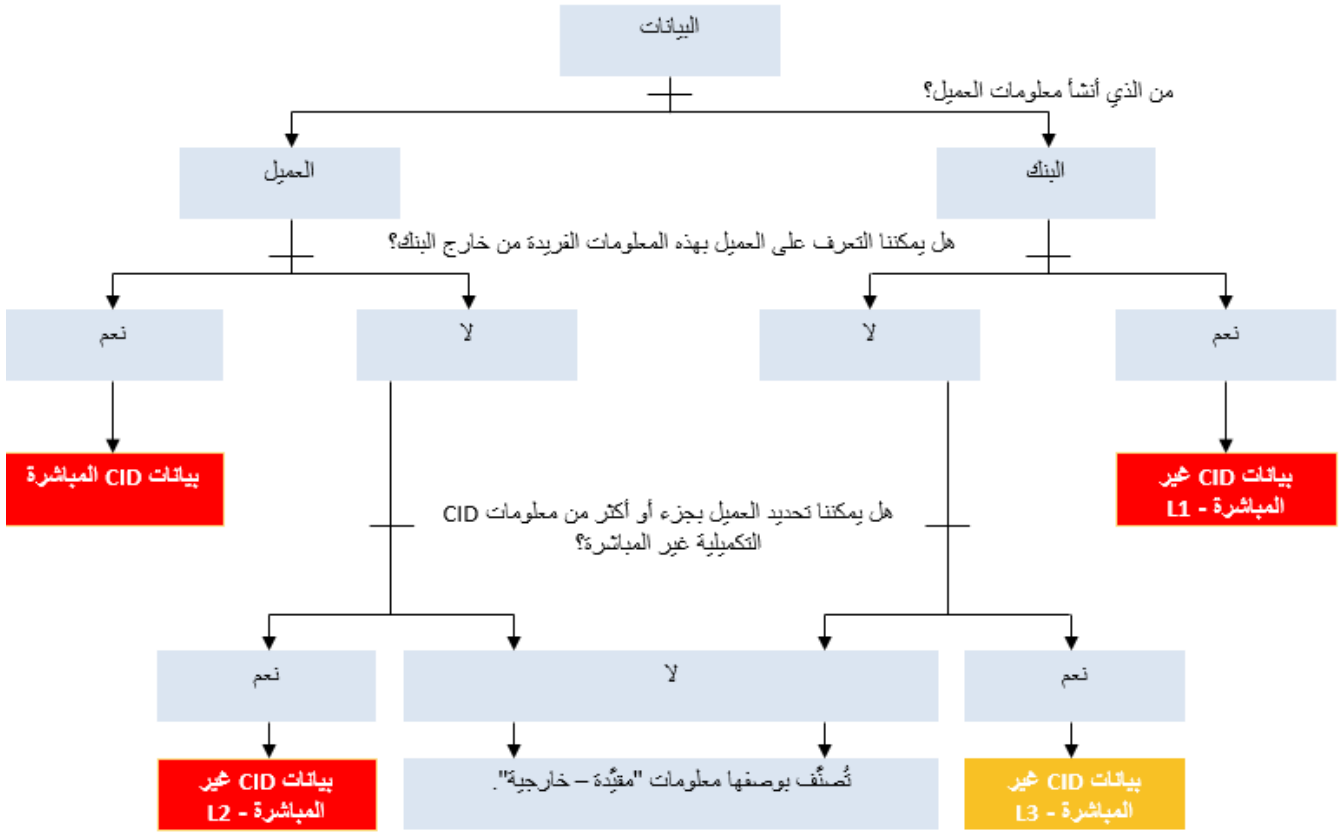
(= DCID) انتهاك السرية البنكية

2. معرف هوية الحاوية

(= L1 DCID) انتهاك السرية البنكية

3. حالة الثروة + الجنسية

انتهاك السرية البنكية = (L2 ICID) + (L2 ICID)


البيانات
من الذي أنشأ معلومات العميل؟
العميل
البنك
هل يمكننا التعرف على العميل بهذه المعلومات الفريدة من خارج البنك؟
نعم
لا
لا
نعم
بيانات CID المباشرة
بيانات CID غير المباشرة - L1
هل يمكننا تحديد العميل بجزء أو أكثر من معلومات CID التكميلية غير المباشرة؟
نعم
لا
نعم
بيانات CID غير المباشرة - L2
تُصنَّف بوصفها معلومات "مقيَّدة – خارجية".
بيانات CID غير المباشرة - L3

الملحق E: مخطط التسميات المعلوماتية لبنك باركليز

الجدول E1: مخطط التسميات المعلوماتية لبنك باركليز

** تختص تسمية "السرية البنكية " بدوائر اختصاص السرية البنكية.

التسمية	التعريف	الأمثلة
السرية البنكية	المعلومات المتعلقة بأي بيانات محددة لهوية العميل (CID) سويسرية سواء أكانت مباشرة أم غير مباشرة. ينطبق تصنيف "السرية البنكية" على المعلومات ذات الصلة بأي بيانات محددة لهوية العميل مباشِرة أو غير مباشِرة. ومن ثم، فإن الوصول من قِبل جميع الموظفين، حتى الموجودين في دائرة الاختصاص المالكة، ليس مناسبًا. يلزم الوصول إلى هذه المعلومات فقط من جانب الذين يحتاجون إلى المعرفة للوفاء بواجباتهم الرسمية أو مسؤولياتهم التعاقدية. قد يترتب على الإفصاح عن هذه المعلومات أو الوصول إليها أو مشاركتها داخل الكيان الخاص بها وخارجه تأثير خطير وقد يؤدي إلى إجراءات جنائية وتكون له عواقب مدنية وإدارية كفرض الغرامات وفقد الترخيص البنكي، في حال الإفصاح عنها لأشخاص غير مصرح لهم في الداخل أو الخارج.	• اسم العميل • عنوان العميل • التوقيع • عنوان IP الخاص بالعميل (ثمة أمثلة إضافية في الملحق D)

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). 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. • معلومات التخطيط الإستراتيجي - التجارية والتنظيمية. • معلومات محددة حول تهيئة أمن نظام المعلومات. • نتائج تدقيق وتقارير محددة. • محاضر اللجنة التنفيذية. • تفاصيل المصادقة أو التعريف والتحقق (ID&V) - الزبون/العميل والزميل. • كميات كبيرة من معلومات حامل البطاقة. • توقعات الأرباح أو النتائج المالية السنوية (قبل نشرها للجمهور). • أي بنود مشمولة باتفاقية عدم إفشاء رسمية (NDA).
مقيَّدة – داخلية	يلزم تصنيف المعلومات بوصفها مقيَّدة - داخلية إذا كان المستلمون المتوقعون هم فقط الموظفون المعتمدون من بنك باركليز وموفرو الخدمات المُدارة (MSP) لبنك باركليز بموجب عقد سارٍ قيد التنفيذ، وكانت تقتصر على جمهور معين.	• الإستراتيجيات والميزانيات. • تقييم الأداء. • رواتب الموظفين وبياناتهم الشخصية. • تقييم مدى التأثر. • نتائج التدقيق والتقارير.

	وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي). ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة.	
مقيَّدة – خارجية	يلزم تصنيف المعلومات بوصفها مقيَّدة - خارجية إذا كان المستلمون المتوقعون هم فقط الموظفين المعتمدين من بنك باركليز وموفِّري الخدمات المُدارة لبنك باركليز بموجب عقد سارٍ قيد التنفيذ، وكانت تقتصر على جمهور معين أو أطراف خارجية مصرح لها من قِبل مالك المعلومات. وسيكون للإفصاح غير المصرح به تأثير سلبي في بنك باركليز، يتم تقييمه بموجب إطار العمل ERMF بوصفه "جسيمًا" أو "محدودًا" (ماليًا أو غير مالي). ولا تكون هذه المعلومات مخصصة للتوزيع العام ولكن يمكن إعادة توجيهها أو مشاركتها من قِبل المستلمين عملاً بمبدأ الحاجة إلى المعرفة.	• خطط منتجات جديدة. • عقود العملاء. • العقود القانونية. • معلومات الأفراد/معلومات زبائن/عملاء الأحجام المنخفضة المقرر إرسالها خارجيًا. • معلومات الزبائن/العملاء. • مواد عرض الإصدار الجديد (مثل نشرة الإصدار، مذكرة العرض). • مستندات البحث النهائية. • المعلومات الجوهرية غير العامة وغير التابعة لبنك باركليز (MNPI). • كل التقارير البحثية • المواد التسويقية المحددة. • تعليقات السوق.
غير مقيدة	المعلومات المعدة للتوزيع العام، أو التي لن يكون لها أي تأثير سلبي في المؤسسة حال توزيعها.	• المواد التسويقية. • المنشورات. • الإعلانات العامة. • إعلانات الوظائف. • المعلومات التي لا تأثير لها في بنك باركليز.

الجدول E2: مخطط التسميات المعلوماتية - متطلبات المعالجة

** متطلبات المعالجة المحددة لبيانات CID لضمان سريتها وفق المتطلبات التنظيمية

مرحلة دورة الحياة	متطلبات السرية البنكية
الإنشاء **التسمية**	وفق "مقيَّدة خارجية" و: • يلزم تعيين مالك للبيانات المحدِّدة لهوية العميل للأصول.

التخزين	وفق "مقيَّدة خارجية" و: • يلزم حصر تخزين الأصول على وسائط قابلة للإزالة طالما كان مطلوبًا صراحة بموجب حاجة تجارية محددة أو من قِبل جهات تنظيمية أو مدققين خارجيين. • يلزم عدم تخزين كميات كبيرة من أصول معلومات السرية البنكية على أجهزة/وسائط محمولة. لمزيد من المعلومات، اتصل بفريق الأمن السيبراني والمعلوماتي المحلي (يشار إليه فيما بعد بالاختصار CIS). • يتعين عدم تخزين الأصول (سواء كانت ورقية أو إلكترونية) بالأماكن التي تحتمل وصول الأفراد غير المصرح لهم إلى تلك الأصول أو اطلاعهم عليها، وفق مبدأ الحاجة إلى المعرفة أو الحاجة إلى الامتلاك. • يلزم اتباع ممارسات مكان العمل الآمنة مثل إخلاء سطح المكتب وقفل شاشة سطح المكتب لحفظ الأصول (سواء أكانت مادية أم إلكترونية). • يلزم استخدام أصول معلومات الوسائط القابلة للإزالة فقط للتخزين طالما كان ذلك مطلوبًا صراحةً، واحتجازها بعيدًا عندما لا تكون قيد الاستخدام. • تتطلب عمليات نقل البيانات المخصصة إلى الأجهزة/الوسائط المحمولة موافقة مالك البيانات وفريق الامتثال وفريق CIS.
الوصول والاستخدام	وفق "مقيّدة خارجية" و: • يلزم عدم إزالة/عرض الأصول خارج الموقع (منشآت بنك باركليز) دون إذن رسمي من مالك بيانات CID (أو من ينوب عنه). • يجب عدم إخراج الأصول/عرضها خارج نطاق ولاية اختصاص حجز العميل دون إذن رسمي من مالك بيانات CID (أو من ينوب عنه) والعميل (تنازل/توكيل محدود). • يجب اتباع ممارسات العمل الآمنة عن بُعد، مع ضمان عدم إمكانية التعرض للتلصص على المستخدم، عند إخراج الأصول المادية من الموقع.
	• التأكُّد من أنَّ الأشخاص غير المصرح لهم لا يمكنهم مراقبة الأصول الإلكترونية التي تحتوي على البيانات المحدِّدة لهوية العميل أو الوصول إليها من خلال استخدام الوصول المقيد إلى تطبيقات الأعمال.
المشاركة	وفق "مقيّدة خارجية" و: • يلزم توزيع الأصول فقط وفق "مبدأ الحاجة إلى المعرفة" وضمن حدود أنظمة معلومات ولاية اختصاص السرية البنكية الأصلية وموظفيها. • تتطلب الأصول التي يتم نقلها على أساس مخصص باستخدام وسائط قابلة للإزالة موافقة مالك أصول المعلومات وفريق CIS. • يجب تشفير الاتصالات الإلكترونية في أثناء النقل. • يلزم تسليم الأصول (الورقية) المرسلة عبر البريد باستخدام خدمة تتطلب إيصال تأكيد استلام. • يلزم أن يقتصر توزيع الأصول فقط على الامتثال "لمبدأ الحاجة إلى المعرفة".
الأرشفة والتخلص	وفق "مقيَّدة خارجية"

*** 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	مقيَّدة – داخلية	مقيَّدة – خارجية	سرية
الإعداد والتقديم	• يلزم تعيين مالك لأصول المعلومات للأصول.	• يلزم تعيين مالك لأصول المعلومات للأصول.	• يلزم تعيين مالك لأصول المعلومات للأصول.
التخزين	• 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). • 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. • 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.	• 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 مخولين عليها. • 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).
الوصول والاستخدام	• يلزم عدم ترك الأصول (سواء أكانت ورقية أم إلكترونية) في أماكن عامة تقع خارج المنشآت. • يلزم عدم ترك الأصول (سواء أكانت مادية أم إلكترونية) في مواقع عامة داخل المنشآت والتي قد يكون للزوار فيها وصول غير خاضع للإشراف. • 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). • يلزم استرداد الأصول المطبوعة على الفور من الطابعة. وفي حال عدم التمكن من ذلك، يلزم الاستعانة بأدوات الطباعة الآمنة. • تلزم حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة.	• 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). • يتعين طباعة الأصول من خلال استخدام أدوات طباعة آمنة. • يتعين حماية الأصول الإلكترونية من خلال ضوابط إدارة الوصول المنطقي المناسبة

المشاركة	• يتعين إرفاق ملصق معلوماتي واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين أن تحتوي الأصول الإلكترونية على ملصق معلوماتي واضح. • 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 معلوماتي واضح على الأصول المطبوعة. كما يتعين أن يكون هذا الملصق على الصفحة الأولى على أقل تقدير. • يتعين إرفاق ملصق معلوماتي واضح على الجانب الأمامي للمغلفات التي تحتوي على أصول مطبوعة • 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 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 معلوماتي واضح على كل صفحة من صفحات الأصول المطبوعة. • 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. • 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 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 أصول 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 وسائط إعلامية, تم تخزين الأصول الإلكترونية السرية عليها, بشكل مناسب وذلك قبل عملية التخلص منها أو خلالها.