الموردين بمراقبة الالتزام (SCO)

الأمن المعلوماتي والسيبراني (ICS)

الإصدار 12.0، أكتوبر 2022

مجال/عنوان الرقابة	وصف الضابط	سبب الأهمية
1. الاستخدام المعتمد	يجب أن ينشر المورّد متطلبات الاستخدام المقبولة لإبلاغ جميع الموظفين العاملين لدى المورّدين بما في ذلك المتعهدون، والمتعهدون من الباطن وجهات معالجة البيانات من الباطن عن مسؤولياتهم. 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 قوات 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 التوافق مع متطلبات الاستخدام المقبول.	يساعد مطلب الاستخدام المقبول على تعزيز بيئة التحكم التي تحمي أصول المعلومات.
2. أمن الحدود والشبكات	يجب أن يضمن المورّد أن تكون كلّ الأنظمة والتطبيقات التي يشغّلها المورّد و/أو متعهدوه من الباطن/جهات معالجة البيانات من الباطن التابعة له التي تدعم خدمات بنك باركليز مشمولة بالحماية ضد تهديدات الشبكة الواردة والصادرة. ويجب تنفيذ الضوابط لضمان أمن المعلومات المخزّنة في الشبكات وحماية الخدمات المتصلة من الوصول غير المصرّح به. يجب على المورّد تحديد أي تنبيهات وأي خروقات أمنية وعليه أن يحمي الأمن وأن يكشف التهديدات والخروقات الأمنية ويستجيب لها. تضمن ضوابط أمان الشبكة حماية المعلومات في الشبكات ومراقبها الداعمة المخصصة لمعالجة المعلومات، ويجب أن تتضمن، على سبيل المثال لا الحصر، المجالات التالية: • الاحتفاظ بقائمة جرد محدَّثة لكل حدود شبكة المؤسسة (من خلال بنية/الرسم التخطيطي للشبكة)، ويجب مراجعتها مرةً واحدةً على الأقل سنويًّا. • توثيق الاتصالات الخارجية بشبكة المورّدين وتوجيهها والتحقُّق منها والموافقة عليها قبل إنشاء الاتصالات لمنع الانتهاكات الأمنية. • تدب حماية شبكات المورّدين من خلال تطبيق مبادئ دفاعية متعمقة (مثل: تجزئة الشبكة، وجدران الحماية، وضوابط الوصول المادي إلى تجهيزات الشبكة، وما إلى ذلك).	إذا لم يتم تنفيذ هذا المبدأ، فقد تتعرَّض الشبكات الخارجية أو الداخلية للإفساد من جانب المهاجمين بهدف الوصول إلى الخدمة أو البيانات الموجودة داخلها.

	• يجب أن تتوفر لدى المورّد تقنيات لمنع التسلل إلى الشبكة بغرض الكشف عن حركة مرور البيانات الضارة ومنعها لكل حركة مرور البيانات الواردة والصادرة، وتحديث قواعد بيانات التوقيعات بما يتوافق مع أفضل الممارسات في المجال وتطبيق التحديثات من موفر الحلول في الوقت المناسب. • استخدام قرات 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. • تتم تقوية أجهزة الشبكة بأمان لمنع أي هجوم ضار. • يجب توثيق كل قواعد التكوين التي تسمح بتدفق حركة مرور البيانات عبر أجهزة الشبكة في نظام إدارة التكوين مع وجود سبب محدد له علاقة بالأعمال لكل قواعد. • الفصل المنطقي لمنافذ/واجهات إدارة الأجهزة عن الشبكة المحلية/حركة مرور البيانات الخاصة بالمستخدم، وضوابط المصادقة المناسبة. • إجراء عمليات مسح منتظمة من خارج كل حد من حدود الشبكة لاكتشاف أي منافذ غير مصرّح بها يمكن الوصول إليها عبر الحدود. • تأمين الاتصالات بين الأجهزة ومحطات/وحدات التحكم بالإدارة. • التأكّد من أن التسجيل والمراقبة يشملان الكشف عن النشاط المشبوه وإطلاق تنبيهات بشأنه (باستخدام السلوك ومؤشرات محفزات الاختراق)، مثل الكشف عن النشاط المشبوه وإطلاق تنبيهات بشأنه عبر SIEM. • 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 على المورّد مراجعة قواعد جدار الحماية (جدار الحماية الخارجي والداخلي) ويجب عليه إخضاعه للمراجعة مرة واحدة سنويًا على الأقل. • يجب على المورّد التأكد من مراقبة الوصول إلى الشبكة الداخلية من خلال ضوابط الوصول إلى الشبكة المناسبة. • يجب السماح للأجهزة المعتمدة فقط (الأجهزة التي توفرها جهة خارجية ذات بنية آمنة وليس منها أي أجهزة بنظام إحضار الأجهزة الشخصية (BYOD)) بالاتصال بشبكة الموردين. • يخضع كل الوصول اللاسلكي إلى الشبكة لبروتوكولات التفويض والمصادقة والتجزئة والتشفير القوية لمنع الانتهاكات الأمنية. • يجب استخدام مصادقة متعددة العوامل عند الوصول عن بُعد إلى شبكة المورّد من خلال تسجيل الدخول. • يجب أن تكون لدى المورّد شبكة (منطقية) منفصلة للخدمة (الخدمات) المقدَّمة إلى بنك باركليز. يجب على المورّد التأكُّد من عدم نشر أي خوادم وتطبيقات مستخدمة لتقديم الخدمة إلى بنك باركليز على شبكات غير موثوق بها (الشبكة التي تقع خارج محيط الأمن الخاص بك، وتلك التي تكون خارجة عن سيطرتك الإدارية، مثل التي تدخل على الإنترنت) من دون ضوابط أمنية مناسبة. يجب على المورّد الذي يتيح استضافة لمعلومات بنك باركليز (بما في ذلك المتعهدون من الباطن وجهات معالجة البيانات من الباطن) في مركز البيانات أو السحابة، أن يكون حاصلاً على شهادة أفضل ممارسة في الصناعة لإدارة أمن الشبكة. **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/الميل الأخير الخاص بالمورّد أو المتصل ببوابات الشبكة الخارجية لبنك باركليز باستخدام مفهوم الحد من ضوابط المنافذ والبروتوكولات والخدمات؛ o التأكّد من أن التسجيل والمراقبة يشملان الكشف عن النشاط المشبوه وإطلاق تنبيهات بشأنه (باستخدام السلوك ومؤشرات محفزات الاختراق)، مثل الكشف عن النشاط المشبوه وإطلاق تنبيهات بشأنه عبر SIEM. **يجب أن يضمن مقدم الخدمات الخارجي تقسيم أي أنظمة أو تطبيقات تقدّم الخدمات التي يعتبرها بنك باركليز ذات مخاطر عالية وتتصل بالبائع الذي يعدُّ ذا مخاطر عالية، إلى مقاطع وفقًا للمبادئ التالية:** i. يجب اتباع نهج التقسيم للحد من التعرض للمخاطر ومنع الحركة الجانبية عبر الشبكة والحد من مخاطر بث الشبكة. يجب نشر التطبيقات على المقاطع المستقلة للمساعدة في الحد من المخاطر بأكبر قدر ممكن ومعقول. مثال: منطقة الدفعات الأكثر سرعة. ii. يجب نشر كل البنى التحتية والبيانات المتعلقة بتطبيق (تطبيقات) الأعمال إلى منطقة تطبيقات آمنة مستقلة قدر الإمكان، كما يجب فصلها عن شبكة بنك باركليز الداخلية باستخدام تقنية إنفاذ معتمدة من CSO (مثل جدران حماية الشبكة وحل التجزئة المعتمَد). ملحوظة – قد تضمن بعض السيناريوهات تقسيم مكونات، مثل التطبيق وقاعدة البيانات عبر مناطق متعددة، على سبيل المثال، حيث تتم الاستفادة من الأنظمة الأساسية المشتركة. يجب تقييم كل تطبيق على حدة، مع تحديد النهج الأكثر ملاءمة والاتفاق عليه مع مستشار أمن الالتزام بمراقبة الموردين (CSO). iii. يجب فصل الخدمات ماديًا أو منطقيًا. يمكن مشاركة بنية الشبكة الأساسية (مثل الكبلات / المحولات) مع التطبيقات والخدمات الأخرى، أي يمكن تحديد المقاطع منطقيًا من دون الحاجة إلى فرض التجزئة عبر الفصل المادي عن بقية شبكة بنك باركليز. iv. يجب أن تقيّد مناطق التطبيق تدفقات حركة مرور البيانات من مناطق أخرى وإليها (بما في ذلك شبكة CIPE الداخلية)، بناءً على تلك المطلوبة لتشغيل الخدمة وأي أدوات إدارة ومراقبة وأمان معتمدة. يجب أن تنص التكوينات على المنافذ والبروتوكولات وعناوين IP المعينة لمسارات الاتصال المسموح بها، ويجب تقييد كل الاتصالات الأخرى بشكل افتراضي. يجب تجنب القواعد التي تحتوي على نطاقات واعتمادها بشكل استثنائي فقط لضمان تمكين الحد الأدنى من متطلبات الاتصال فقط. v. يجب فصل الحاويات بقوة مع وجود عناصر تحكم منطقية قوية تمنع الحركة الجانبية بين الحاويات، وبالتالي تفرض الفصل. يجب ألا يؤدي اختراق حاوية واحدة إلى تعرّض حاويات أخرى تعمل على المضيف/المجموعة نفسها للاختراق. vi. يجب أن توفر كل عمليات تطبيق التقسيم إمكانية إدارة سياسات مركزية من خلال الوظائف (أو التكامل) للتحقق من توافق السياسة والإبلاغ عن خروقاته (راجع مستند توافق جدار الحماية) وتوفير سجل تغييرات قابل للتدقيق. vii. يجب تشغيل الفحص/أدوات التحكم الملائمة متى أمكن/كان ذلك ممكنًا. viii. يجب تشغيل إمكانات التقسيم بطريقة "آمنة من التعطل"، على سبيل المثال، إذا حدث عطل في الإمكانات، يجب أن تظل مجموعات القواعد المعتمدة لحظر/السماح بحركة مرور البيانات قيد التشغيل. ix. يجب السماح بأي حركة مرور بيانات بين الأنظمة الإنتاجية والأنظمة غير الإنتاجية في مناطق التطبيق فقط عن طريق الاستثناء ويجب تسجيلها. **إرشادات خاصة بعميل (مورّد) خدمة السحابة الذي تتم الاستعانة به لتقديم الخدمة (الخدمات) إلى بنك باركليز** يتعيّن على عميل خدمة السحابة (CSC) ضمان تنفيذ الضوابط المناسبة لأمن الشبكة لحماية خدمة بنك باركليز -	

	• يجب أن يحدد عميل خدمة السحابة متطلباته لفصل الشبكات بهدف تحقيق الفصل بين المستأجرين في البيئة المشتركة لخدمة السحابة والتحقق من أن مقدم خدمة السحابة يلبي هذه المتطلبات. • يجب أن تحدد سياسة التحكم بالوصول التي يحددها عميل خدمة السحابة والخاصة باستخدام خدمات الشبكة متطلبات وصول المستخدم إلى كل خدمة سحابة منفصلة يتم استخدامها. *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 الشبكة التابعة للمتعهد من الباطن التابع للمورّد.*	
3. اكتشاف حجب الخدمة	يجب أن يحتفظ المورّد بإمكانية اكتشاف هجمات حجب الخدمة (DoS) وحجب الخدمة الموزعة (DDoS) والحماية منها. ويجب على المورد التأكد من أن القنوات المتصلة بالإنترنت أو القنوات الخارجية التي تدعم الخدمات المقدمة إلى بنك باركليز يجب أن تحظى بحماية كافية ضد هجمات حجب الخدمة (DoS) لضمان توافرها. إذا كان المورّد يستضيف **الأنظمة والتطبيقات التي توفر الخدمات** ويحتفظ ببيانات بنك باركليز أو يدعم الفئة 0 أو 1 لمرونة الخدمة، يجب أن يكون لهذا الأمر حماية كافية ضد DOS لضمان التوافر.	إذا لم يتم تنفيذ هذا المبدأ، قد يتعذر على بنك باركليز ومورّده منع هجوم حجب الخدمة من تحقيق هدفه.
4. العمل عن بُعد (الوصول عن بُعد)	**الوصول عن بُعد إلى شبكة بنك باركليز** لا يتم توفير الوصول عن بُعد إلى شبكة بنك باركليز عبر تطبيق Citrix الخاص بالبنك المذكور بشكل افتراضي. للوصول إلى شبكة بنك باركليز من مواقع غير معتمدة/خارج المكتب/من المنزل، وأي وصول عن بُعد، يجب الحصول على موافقة مسبقة وتفويض من بنك باركليز (مكتب الأمن الرئيس – فريق ECAM) (externalcyberassurance@barclayscorp.com). يجب على المورّد ضمان إنشاء الضوابط الآتية للوصول عن بُعد: • يجب تشفير تسجيل الدخول عن بُعد إلى شبكة المورّد بتشفير قوي ويجب استخدام المصادقة المتعددة العوامل. • يلزم أن يكون الوصول إلى شبكة بنك باركليز عبر تطبيق Barclays Citrix باستخدام رمز التشفير باستخدام مفتاح عام (RSA) (الجهاز والبرنامج) المقدم من بنك باركليز • يجب على المورّد الاحتفاظ بقائمة جرد بكل رموز RSA المميزة (المكونة من أجهزة وبرامج) التي يقدمها بنك باركليز. يجب دعم استخدام الرموز المميزة بواسطة عملية إدارية. يجب أن تتضمن العملية مراجعة تخصيص الرموز المميزة ومراقبتها، وفقدانها/سرقتها، واستخدامها وإعادتها (الرمز المميز المادي). • يجب أن يحتفظ المورد بسجل حديث وصحيح لموظفيه الذين تمت الموافقة على عملهم عن بُعد مع تقديم مبرر للأعمال لكلّ موظف معتمد، بما في ذلك المتعهد من الباطن/جهات معالجة البيانات من الباطن. • **يجب على المُورّد إجراء تسوية لجميع الموظفين المعنيين بالوصول عن بُعد كل ثلاثة أشهر، على أن يلي ذلك إبلاغ بنك باركليز عن نتائجه (مكتب الأمن الرئيس - فريق ECAM) (externalcyberassurance@barclayscorp.com).** • سيلغي بنك باركليز تنشيط بيانات اعتماد المصادقة عند الإخطار بأنه لم تعُد هناك حاجة إلى الوصول (كأن يتم إنهاء عمل الموظف، أو إعادة تعيين المشروع، أو ما إلى ذلك) **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).	تساعد ضوابط الوصول عن بُعد على ضمان عدم اتصال الأجهزة غير المصرح لها وغير الآمنة ببيئة بنك باركليز عن بُعد.

	• يجب على المورّد التأكد من ضرورة التكوين الآمن لنقطة النهاية المستخدمة لربط أنظمة معلومات بنك باركليز عن بُعد (مثل: مستوى التصحيح، أو حالة مكافحة البرامج الضارة، أو ماذلك). • 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 - externalcyberassurance@barclayscorp.com). يتعين على المورد الاحتفاظ بالسجلات وإجراء التسوية على أساس ربع سنوي. • **يجب عدم السماح للأجهزة الشخصية/الأجهزة القائمة على إستراتيجية جلب الجهاز الشخصي (BYOD) بالوصول إلى بيئة بنك باركليز و/أو بيانات بنك باركليز الموجودة/المخزنة في بيئة يديرها المورّد (التي تشمل موظفي المورد واستشاريه وعمال الطوارئ والمتعهدين وشركاء الخدمة المدارة والمتعهدين من الباطن/جهات معالجة البيانات من الباطن).** ملحوظة: لا يُسمح بالوصول عن بعد إلى شبكة بنك باركليز وبيانات بنك باركليز ما لم تتم المواقة عليه والتصريح به بشكل خاص من جانب بنك باركليز. **الوصول عن بُعد إلى بيانات بنك باركليز في بيئة/شبكة المورّد** لا يتم توفير الوصول عن بُعد إلى بيانات بنك باركليز الموجودة/المخزنة و/أو التي تتم معالجتها في بيئة مُدارة بواسطة المورّد بشكل افتراضي. يجب أن يطلب المُورّد تفويضًا من بنك باركليز (مكتب الأمن الرئيس - فريق ECAM - externalcyberassurance@barclayscorp.com) للوصول إليها من مواقع غير معتمدة/خارج المكتب/من المنزل. • يجب تشفير الوصول إلى شبكة المورّد عن بُعد عبر تسجيل الدخول تشفيرًا فائقًا في أثناء نقل البيانات واستخدام المصادقة المتعددة العوامل. • يجب على المورد الاحتفاظ بسجلات للأفراد الذين كانوا يعملون عن بُعد والأسباب المنطقية وراء الوصول عن بُعد. • **يجب على المورد إجراء تسوية لجميع المستخدمين الذين يعملون عن بُعد كل ثلاثة أشهر** • سيلغي المورّد تنشيط بيانات اعتماد المصادقة عندما لا تعود ثمة حاجة إلى الوصول (كأن يتم إنهاء عمل الموظف، إعادة تعيين المشروع، إلخ) **في غضون أربع وعشرين (24) ساعة.** • يتعين على المورد التأكد من ضرورة التكوين الآمن لنقطة النهاية المستخدمة لربط بيانات بنك باركليز عن بُعد (مثل: مستوى التصحيح، حالة مكافحة البرامج الضارة، إلخ). • **يجب عدم السماح للأجهزة الشخصية/الأجهزة القائمة على إستراتيجية جلب الجهاز الشخصي (BYOD) بالوصول إلى بيانات بنك باركليز الموجودة/المخزنة في بيئة يديرها المورّد (التي تشمل موظفي المورّد واستشاريه وعمل الطوارئ والمتعهدين وشركاء الخدمة المُدارة).**	
5. إدارة سجلات الأمان	يجب أن يضع المُورّد إطار عمل معتمدًا ومُدارًا ومؤسسًا بشكل جيد ومدعومًا لمراجعة الحسابات وإدارة السجلات. يجب أن يتضمن إطار العمل أنظمة تكنولوجيا المعلومات الرئيسية، بما في ذلك التطبيقات وأجهزة الشبكات وأجهزة الأمن والخوادم التي تم تعيينها لتسجيل الأحداث الرئيسية. يجب أن يتأكد المورد من أن السجلات يتم التعامل معها بشكل مركزي، وأنها مؤمّنة بشكل مناسب ضد التلاعب و/أو الحذف، وأن المورد يحتفظ بها لمدة لا تقل عن 12 شهرًا أو للمدة التي تحددها المتطلبات التنظيمية، أيهما أكبر.	إذا لم يتم تنفيذ هذا الضابط، فلن يتمكن المورّد من اكتشاف الاستخدام غير الملائم أو الضار لخدمته أو بياناته والاستجابة له في غضون قترات زمنية معقولة.

الفئة	أنظمة/خدمات منخفضة التأثير	أنظمة/خدمات متوسطة التأثير	أنظمة/خدمات عالية التأثير
الاحتفاظ بالسجلات	3 أشهر	6 أشهر	12 شهرًا

يجب أن يتناول إطار عمل إدارة سجلات الأمن الجوانب 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 في مراقبة الهجوم أو الكشف عنه أو فهمه أو التعافي منه أو كل ما سبق، 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، وبرنلمج 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.
- 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 متعدد الأوجه ومنعها بصورة أفضل.
- يجب أن تتضمن الأحداث الرئيسية التي يتم تسجيلها تلك الأحداث التي من المحتمل أن تؤثر في سرية الخدمات المقدمة إلى بنك باركليز وسلامتها ومدى توافرها، والتي قد تساعد في تحديد الحوادث و/أو انتهاكات حقوق الوصول التي تحدث في ما يتعلق بأنظمة المورّد أو التحقيق فيها.

	• عليك المداومة على إجراء اختبار للتحقق من أن إطار العمل لا يزال يفي بالمتطلبات المذكورة أعلاه. **إرشادات خاصة بعميل (مورّد) خدمة السحابة الذي تتم الاستعانة به لتقديم الخدمة (الخدمات) إلى بنك باركليز** يجب على عميل خدمة السحابة (CSC) ضمان تطبيق الضوابط المناسبة لإدارة سجل الأمان لحماية خدمة بنك باركليز - • يجب أن يحدد عميل خدمة السحابة متطلبات تسجيل الأحداث ويوثقها، وأن يتحقق من أن خدمة السحابة تستوفي هذه المتطلبات. • إذا تم تفويض عملية مميزة إلى عميل خدمة السحابة، يجب تسجيل تشغيل هذه العمليات وأداؤها. يجب أن يحدد عميل خدمة السحابة ما إذا كانت إمكانات التسجيل التي يوفرها موفر مقدم خدمة السحابة مناسبة أم أنه يجب على عميل خدمة السحابة تطبيق إمكانات تسجيل إضافية. • يجب أن يطلب عميل خدمة السحابة معلومات حول مزامنة الساعة المستخدمة لأنظمة مقدم خدمة السحابة. • يجب أن يطلب عميل خدمة السحابة معلومات من مقدم خدمة السحابة حول إمكانات مراقبة الخدمة المتوفرة لكل خدمة سحابة.	
6. التصدي للبرامج الضارة	تماشيًا مع أفضل ممارسة في الصناعة، يجب أن يكون المورّد قد وضع سياسات وإجراءات راسخة، ما يؤدي إلى دعم العمليات التجارية والتدابير التقنية المنفذة، لمنع تنفيذ البرامج الضارة في 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. يجب 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. • التأكد من أن برنامج الحماية من البرامج الضارة في المؤسسة يقوم بتحديث محرك الفحص الخاص به • تحديث قاعدة بيانات التوقيعات بشكل منتظم • إرسال كل أحداث الكشف عن البرامج الضارة إلى أدوات إدارة مكافحة البرامج الضارة وخوادم سجلات الأحداث لدى المؤسسة للتحليل والتنبيه. • يجب على المورّد تطبيق الضوابط المناسبة للحماية من البرامج الضارة والهجمات على الأجهزة المحمولة المُستخدمة في خدمات بنك باركليز. 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.
7. معايير التكوين الآمن	يجب أن يكون لدى المورّد إطار عمل راسخ لضمان تكوين كل الأنظمة القابلة للتكوين و/أو 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

	• إجراء فحوصات إنفاذ منتظمة (سنويًا على الأقل) لضمان التصحيح الفوري لعدم التوافق مع معايير الأمن الأساسية. تطبيق عمليات فحص ومراقبة مناسبة لضمان 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). • إجراء تدقيق دوري في التكوين سنويًا على الأقل لضمان عدم وجود أي تكوين غير مصرح به في بيئة الإنتاج الفعلية. • التأكُّد من أنَّ إدارة التكوين تحكم معايير التكوين الآمن عبر جميع فئات الأصول، وتكتشف تغييرات التهيئة أو الانحرافات وتنبه بها وتستجيب لها بفعالية. **إرشادات خاصة بعميل (مورّد) خدمة السحابة الذي تتم الاستعانة به لتقديم الخدمة (الخدمات) إلى بنك باركليز** يجب على عميل خدمة السحابة (CSC) ضمان تنفيذ ضوابط تكوين آمن مناسبة لحماية خدمة بنك باركليز - • عند تكوين الأجهزة الافتراضية، يجب أن يضمن عملاء خدمة السحابة تعزيز الجوانب المناسبة (على سبيل المثال، تلك المنافذ والبروتوكولات والخدمات المطلوبة فقط)، وأن يتم تطبيق التدابير التقنية المناسبة (مثل الحماية من البرامج الضارة والتسجيل) لكل جهاز افتراضي مُستخدَم.	التغييرات على ضمان حماية أصول معلومات بنك باركليز.
8. أمن نقطة النهاية	يجب على المورّد تبني نهج إدارة نقاط نهاية موحّد للتأكُّد من ضرورة تقوية نقاط النهاية المُستخدمة للوصول إلى شبكة بنك باركليز، أو الوصول إلى أصول معلومات/بيانات بنك باركليز أو معالجتها، أو القيام بكلّ من الأمرين، من أجل توفير الحماية ضد أي هجمات ضارة. يجب أن تكون أفضل الممارسات في الصناعة قيد التطبيق، كما يجب أن يتضمن إنشاء أمان نقاط النهاية، على سبيل المثال لا الحصر، ما يأتي: • تشفير القرص الصلب بالكامل. • تعطيل جميع البرامج/الخدمات/المنافذ غير المطلوبة. • تعطيل الوصول إلى حقوق الإدارة للمستخدم المحلي. • عدم السماح للموظف التابع للمورّد بتغيير الإعدادات الأساسية مثل: حزمة الخدمة الافتراضية وقسم النظام والخملت الافتراضية ومكافحة الفيروسات، وما إلى ذلك. • تعطيل منفذ USB المستخدم لنسخ معلومات/بيانات بنك باركليز إلى وسائط خارجية • 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 خيار "تعطيل الوصول إلى الطابعة" بشكل افتراضي. • يجب أن يضمن المورّد حظر ترشيح بيانات بنك باركليز إلى مواقع الشبكات الاجتماعية وخدمات بريد الويب والمواقع التي يمكن أن تخزّن المعلومات، مثل Google Drive وDropbox وiCloud على سبيل المثال لا الحصر. • تعطيل مشاركة/إرسال بيانات بنك باركليز باستخدام أدوات/برامج المراسلة الفورية. • الكشف عن حالة وجود و/أو استخدام برامج غير مصرح بها، بما في ذلك البرامج الضارة، وإيقافها ومعالجتها. ملحوظة: ينبغي تعطيل الوسائط القابلة للإزالة/الأجهزة المحمولة بصورة افتراضية وتمكينها فقط للأسباب التجارية المشروعة.	إذا لم يتم تنفيذ هذا الضابط، فقد تكون نقاط النهاية والشبكة الخاصة ببنك باركليز والمورّد عُرضة للهجمات السيبرانية.

	يجب أن يحتفظ المورّد بصور أو قوالب آمنة لكل الأنظمة في أي مؤسسة بناءً على معايير التكوين المعتمدة في المؤسسة. يجب تكوين أي نشر لنظام جديد أو أي نظام موجود تم 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 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 تطبيقات Citrix الخاصة ببنك باركليز. إذا تعذر على المورّد تثبيت أداة تحليل نقطة النهاية أو استخدامها، فلا بد من إخطار مدير العلاقات في بنك باركليز بذلك. الأجهزة المحمولة المستخدمة في خدمات بنك باركليز - • يجب على المورّد التأكُّد من تطبيق إمكانات إدارة نقطة النهاية الموحّدة (UEM) أو 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. • يجب أن يضمن المورد توفر إمكانات قفل الجهاز المحمول ومسح بياناته عن بُعد واستخدامها لحماية المعلومات في حال فُقد الجهاز أو سرقته أو اختراقه. • تشفير بيانات بنك باركليز المخزّنة و/أو المعالجة على بيانات الجهاز المحمول	
9. منع تسرب البيانات	يجب على المُورّد استخدام إطار عمل فعّال معتمد من الإدارة لتأمين بيانات بنك باركليز من التسرّب/الترشيح، بما في ذلك على سبيل المثال لا الحصر قوات تسريب البيانات: - • 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 الجهات الخارجية (المتعهدون من الباطن وجهات معالجة البيانات 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، قد 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
10. أمان البيانات	يجب على المُورّد تأمين بيانات بنك باركليز التي يحتفظ بها و/أو تتم معالجتها من خلاله عبر مجموعة من تقنيات التشفير وحماية النزاهة ومنع فقدان البيانات. يجب أن يقتصر الوصول إلى بيانات بنك باركليز على موظفها المخوّل فقط وأن يكون محميًا من الإصابة بالفيروسات وهجمات التجميع وهجمات الاستدلال وتهديدات التخزين، بما في ذلك على سبيل المثال لا الحصر التهديدات الصادرة من بيئات الحوسبة السحابية. ينبغي أن تتضمن ضوابط أمان البيانات، على سبيل المثال لا الحصر، المجالات الآتية: 1. يلتزم المورّد في كل الأوقات بالتوافق مع القوانين المعمول بها لحماية البيانات، منفردةً أو مجتمعةً.	

	2. وضع السياسات والعمليات والإجراءات، ما يدعم العمليات التجارية والتدابير التقنية. توثيق تدفقات البيانات والاحتفاظ بها بالنسبة إلى البيانات الموجودة في الموقع الجغرافي للخدمة (الفعلي والاقتراضي). يجب أن يشمل ذلك التفاصيل المرتبطة بجزء مكونات التطبيقات والأنظمة في تدفق البيانات. 3. الاحتفاظ بمخطط تدفق البيانات الخاص ببيانات بنك باركليز الموجودة ضمن المواقع الجغرافية (بما في ذلك المواقع المادية والاقتراضية) في التطبيقات ومكونات النظام. 4. الاحتفاظ بقائمة جرد لكل المعلومات الحساسة/السرية الخاصة ببنك باركليز، والتي يقوم المورّد بتخزينها أو معالجتها أو إرسالها. 5. التأكُّد من تصنيف كل بيانات بنك باركليز ووضع علامة عليها استنادًا إلى معيار تصنيف المعلومات وحمايتها المُعتمد من الإدارة. 6. حماية البيانات في أثناء عدم النقل؛ a. تشفير البيانات تشفيرًا فائقًا في أثناء عدم نقلها لمنع الكشف عن أصول معلومات بنك باركليز 7. مراقبة نشاط قاعدة البيانات؛ a. مراقبة الوصول إلى قاعدة البيانات والنشاط وتسجيله لتحديد النشاط الضار بسرعة وفاعلية. 8. حماية البيانات قيد الاستخدام؛ a. توفير ضوابط إمكانية إدارة الوصول لمعالجة المعلومات الحساسة بهدف توفير الحماية 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 في أثناء النقل؛ a. الاستفادة من إمكانات التشفير القوية لضمان حماية البيانات في أثناء النقل. b. يتحقق عادة تشفير البيانات بشكل قوي في أثناء النقل باستخدام تشفير النقل أو الحمولة (حقل مراسلة أو حقل انتقائي). تتضمن آليات تشفير النقل على سبيل المثال لا الحصر: 10. أمان طبقة النقل (باتباع أفضل ممارسة في الصناعة للتشفير الحديث، بما في ذلك استخدام/رفض البروتوكولات والشفرات) 11. الاتصال النفقي الآمن (حزمة بروتوكول الإنترنت الأمنية (IPsec)) 12. بروتوكول النقل الآمن (SSH) a. يلزم تكوين بروتوكولات أمن النقل لمنع التفاوض بشأن الخوارزميات الأضعف و/أو أطوال المفاتيح الأقصر، عندما تدعم كلتا نقطتي النهاية الخيار الأقوى. 13. النسخ الاحتياطي للبيانات – a. يجب وضع أحكام لضمان نسخ البيانات والمعلومات احتياطيًا بصورة ملائمة ومن ثم تكون قابلة للاسترداد (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 و/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. d. عندما يوفّر مقدم خدمة السحابة إمكانية النسخ الاحتياطي في إطار خدمة السحابة، يجب أن يطلب عميل خدمة السحابة مواصفات إمكانية النسخ الاحتياطي من مقدم خدمة السحابة. يجب أن يتحقق عميل خدمة السحابة أيضًا من أنها تفي بمتطلبات النسخ الاحتياطي. يتحمل عميل خدمة السحابة مسؤولية تنفيذ إمكانات النسخ الاحتياطي عندما لا يقوم مقدم خدمة السحابة بتوفيرها.	

11. أمن برامج التطبيقات	يلتزم المورد باستحداث التطبيقات باستخدام ممارسات التشفير الآمنة وفي بيئة آمنة. عندما يطور المورّد تطبيقات للاستخدام بواسطة بنك باركليز، أو تُستخدم لدعم الخدمة المقدمة إلى بنك باركليز، يجب على المُورّد إنشاء إطار تطوير برنامج آمن لدمج الأمن في دورة تشغيل تطوير البرامج. يجب على المورّد اختبار نقاط الضعف في البرنامج ومعالجتها قبل تسليمها إلى بنك باركليز. ينبغي أن يتضمن أمان برامج التطبيق، على سبيل المثال لا الحصر، المجالات الآتية: • وضع معايير ترميز آمنة ومُعتمدة من الإدارة وتبنيها بما يتسق مع أفضل ممارسات الصناعة لمنع نقاط الضعف وانقطاع الخدمة. • 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. • تطبيق 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. • يجب على المورد ضمان عدم استخدام البيانات المباشرة (ومنها المعلومات الشخصية) في البيئات غير الإنتاجية. • يجب تصميم واجهات التطبيقات والبرامج (API) واستحداثها ونشرها واختبارها وفق أفضل ممارسة في الصناعة (مثل: OWASP لتطبيقات الويب). • حظر استخدام مستودعات الترميز العام 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 تطبيقات خاصة إذا كانت هذه الأدوات متاحة لنوع التطبيق. 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 ممكنًا، فسيجب نشر جدار حماية تطبيق الويب المستند إلى المضيف.	تساعد الضوابط التي تحمي استحداث التطبيقات على ضمان تأمين التطبيقات عند النشر.
12. إدارة الوصول المنطقي (LAM)	يجب تقييد الوصول إلى المعلومات وأن يكون تحت توجيه، مع المراعاة الواجبة لمبادئ 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.

	• 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 يحتاجون إلى 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 تنفيذ إدارة دورة الحياة لحقوق الوصول بما في ذلك تحديد الهوية والمصادقة والتفويض. يجب لإدارة حقوق الوصول المنطقية والتفويض أن يضمنا أن تشمل عملية منح الوصول وتعديله وإلغائه مستوى التفويض المناسب للامتيازات التي تم منحها. • يجب الالتزام بالضوابط المعمول بها للتأكُّد من اشتمال عمليات إدارة الوصول على الآليات اللازمة للتحقق من الهوية. • يجب ربط حساب فريد بفرد واحد، ويكون 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. • يجب مراجعة كل أذونات الوصول المميزة كل ستة (6) أشهر على الأقل. يجب أن تكون إدارة الامتيازات متوافقة مع إدارة الوصول المميز (PAM) الفعالة. • يجب ضم بيانات الاعتماد غير الشخصية (أي كلمات المرور والأسرار) إلى أداة مناسبة تتوافق مع أفضل معايير الصناعة التي توفر الضمان السرية والنزاهة والتوافر (CIA) لتوفير إمكانات بيانات الاعتماد/منح الوصول السريع والمحدود في وقت الحاجة. وفي حال تعذر ذلك، يجب تأمين بيانات الاعتماد بحيث لا يستطيع أي إنسان استخدامها. عندما يكون الاستخدام البشري للحساب مطلوبًا، يجب أن يكون الوصول مؤقتًا ومرتبطًا بوقت، وتجب إعادة تعيين بيانات الاعتماد بعد ذلك، ويُشار إلى ذلك عادةً باسم "منح الوصول السريع والمحدود في وقت الحاجة". مصطلح "منح الوصول السريع والمحدود في وقت الحاجة" داخل الحوسبة يُستخدم لوصف عملية التحقق من كلمة مرور حساب النظام للاستخدام بواسطة مستخدم بشري. وهو يُستخدم بشكل عام لحسابات النظم ذات المستوى الأعلى مثل الحساب الجذر في نظام التشغيل Unix أو SYS/SA لقواعد البيانات. تتمتع هذه الحسابات بامتيازات عالية ولا تكون مخصصة في حد ذاتها لإنسان بعينه، ومن ثمّ يقوم منح الوصول السريع والمحدود في وقت الحاجة إلى الحسابات بتقييدها بمدة كلمة المرور، والهدف من ذلك التحكم في استخدام الحساب وتقليله ليقتصر على حالات الضرورة. • عناصر التحكم في المنتقل – إزالة إمكانية الوصول لضمان عدم توفر إمكانية الوصول من إغلاق التشغيل/نهاية الحركة/يوم النقل.	تساعد ضوابط إدارة الوصول على التأكُّد من أنَّ الوصول إلى أصول المعلومات غير متاح سوى للمستخدمين الذين تمت الموافقة عليهم.

	• عناصر التحكم في المغادر – إلغاء كل إمكانية وصول منطقية مستخدمة للوصول إلى موارد معلومات بنك باركليز و/أو تقديم الخدمات إلى بنك باركليز منذ **تاريخ الخروج/يوم العمل الأخير** مع المُورّد. • المصادقة - يجب اتباع طول كلمة المرور ودرجة تعقيدها المناسبَين، أو سجل كلمات المرور، أو تكرار تغيير كلمات المرور، أو المصادقة المتعددة العوامل، أو الإدارة الآمنة لبيانات اعتماد كلمة المرور أو غيرها من عناصر التحكم الأخرى وفق أفضل ممارسة في الصناعة. • 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. • يجب تغيير كلمات المرور إلى 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. **إرشادات خاصة بعميل (مورّد) خدمة السحابة الذي تتم الاستعانة به لتقديم الخدمة (الخدمات) إلى بنك باركليز** يتعيّن على عميل خدمة السحابة (CSC) ضمان تطبيق ضوابط التحكم في الوصول المنطقية المناسبة لحماية خدمة بنك باركليز - • يجب أن يستخدم عميل خدمة السحابة تقنيات مصادقة كافية (على سبيل المثال، المصادقة المتعددة العوامل) للمصادقة على وصول مسؤولي خدمة السحابة لدى عميل خدمة السحابة إلى الإمكانات الإدارية لخدمة السحابة وفقًا للمخاطر المحددة. • يجب أن يضمن عميل خدمة السحابة تقييد الوصول إلى المعلومات في خدمة السحابة بما يتوافق مع سياسة التحكم بالوصول الخاصة به، ووضع هذه القيود موضع التنفيذ. يشمل ذلك تقييد الوصول إلى خدمات السحابة ووظائف خدمة السحابة وبيانات عملاء خدمة السحابة المحفوظة في الخدمة. • عند السماح باستخدام برامج الأدوات المساعدة، يجب على عميل خدمة السحابة تحديد برامج الأدوات المساعدة التي سيتم استخدامها في بيئة الحوسبة السحابية لديه، وضمان عدم تأثيرها على ضوابط خدمة السحابة.	
13. إدارة نقاط الضعف	يجب أن يدير المورّد برنامجًا فعالاً لإدارة نقاط الضعف من خلال السياسات والإجراءات المعمول بها، ودعم العمليات/التدابير التنظيمية، والتدابير التقنية، من أجل المراقبة الفعالة، واكتشاف نقاط الضعف ومعالجتها في الوقت المناسب داخل التطبيقات، وشبكة البنية التحتية، ومكونات النظام المملوكة أو المُدارة بواسطة المورّد لضمان فعالية 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. • يجب على مقدم الخدمة إجراء عمليات فحص لنقاط الضعف بصفة روتينية باستخدام توقيعات نقاط الضعف المحدّثة (بمعدل انتظام مطابق لما تفرضه أفضل ممارسة في الصناعة)، وتُحدِّد هذه العمليات نقاط الضعف المؤكدة وغير المؤكدة بفاعلية عبر كل فئات الأصول داخل البيئة. • الاستفادة من عملية تصنيف المخاطر لتحديد أولويات معالجة نقاط الضعف المكتشفة.	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.

- يجب ضمان معالجة نقاط الضعف بفعالية من خلال أنشطة المعالجة القوية وإدارة التصحيح لتقليل مخاطر استغلال نقاط الضعف (إجراء المعالجة في الوقت المناسب ووفقَ أفضل ممارسة في الصناعة/أو باستخدام برنامج إدارة التصحيح).
- استحداث عملية للتحقق من إصلاح الثغرات التي تتحقق بسرعة وفعالية من معالجة الثغرات عبر جميع فئات الأصول داخل البيئة.
- المقارنة بانتظام بين نتائج عمليات المسح المتتالية لنقاط الضعف، وذلك للتحقُّق من أنَّ نقاط الضعف قد تم علاجها في الوقت المناسب.

بالنسبة إلى خدمات المورّدين المرتبطة **بالبنية الأساسية/تطبيقات الاستضافة** بالنيابة عن بنك باركليز (بما في ذلك **الجهات الخارجية العالية المخاطر** التي تم الإبلاغ عنها)

- 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).

الأولوية	التصنيف	أيام الغلق (الحد الأقصى)
P1	حرج	15
P2	عالٍ	30
P3	متوسط	60
P4	منخفض	180
P5	معلوماتي	360

يجب إبلاغ/إخطار بنك باركليز فورًا بكل المشكلات ونقاط الضعف التي قد يكون لها تأثير مادي في البنية الأساسية/تطبيقات الاستضافة الخاصة ببنك باركليز والمقدمة من المورّد، التي قرر المورّد قبول المخاطرة بها، ومن ثم الحصول على موافقة بنك باركليز عليها كتابيًا (مكتب الأمن الرئيس - فريق ECAM-externalcyberassurance@barclayscorp.com).

إرشادات خاصة بعميل (مورّد) خدمة السحابة الذي تتم الاستعانة به لتقديم الخدمة (الخدمات) إلى بنك باركليز

يتعيّن على عميل خدمة السحابة (CSC) ضمان تطبيق الضوابط المناسبة لإدارة نقاط الضعف لحماية الخدمة المقدمة إلى بنك باركليز -

- يجب أن يطلب عميل خدمة السحابة معلومات من مقدم خدمة السحابة حول إدارة نقاط الضعف التقنية التي يمكن أن تؤثر في خدمات السحابة المقدمة. يجب أن يحدد عميل خدمة السحابة نقاط الضعف التقنية التي سيكون مسؤولاً عن إدارتها، وأن يعرّف بوضوح عمليةً لإدارتها.

<table>
<tr>
<td>14. إدارة التصحيح</td>
<td>يجب على المورّد امتلاك برنامج إدارة تصحيح تدعمه سياسات وإجراءات، وعمليات تجارية/تدابير تنظيمية داعمة، وتدابير تقنية راسخة، وذلك لمراقبة/تتبع الحاجة إلى التصحيح ونشر تصحيحات الأمان لإدارة بيئة/ممتلكات المورّد بالكامل.
يجب أن يضمن المُورّد تحديث الخوادم وأجهزة الشبكة والتطبيقات وأجهزة نقاط النهاية بأحدث تصحيحات الأمان وبما يتوافق مع أفضل الممارسات في المجال، ما يضمن ما يلي:
• ينبغي للمورّد تقييم كل التصحيحات واختبارها 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 تصحيحي. إذا تعذر تصحيح النظام، فقم بنشر التدابير المضادة المناسبة.
• يجب تسجيل كل تغييرات تكنولوجيا المعلومات الرئيسة قبل التنفيذ وكذلك اختبارها والموافقة عليها من خلال عملية إدارة تغييرات قوية ومعتمدة لدعم متطلبات عمليات التدقيق والتحقق واستكشاف الأخطاء وإصلاحها والتحليل في المستقبل.
• يجب على المورّد التحقق من انعكاس التصحيحات على بيئتَي الإنتاج والتعافي من الكوارث (DR).</td>
<td>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.</td>
</tr>
<tr>
<td>15. محاكاة التهديد/اختبار الاختراق/تقييم أمن تكنولوجيا المعلومات</td>
<td>يتعين على المورد التعامل مع مقدم خدمة 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 نقاط الضعف التي يمكن استغلالها والتي تؤدي إلى انتهاك أمان 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 المورّدين المرتبطة بالبنية الأساسية/تطبيقات الاستضافة بالنيابة عن بنك باركليز (بما في ذلك الجهات الخارجية العالية المخاطر التي تم الإبلاغ عنها)
• 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.
• يجب على المورّد مشاركة أحدث تقرير تقييم أمان بصفة سنوية مع بنك باركليز (مكتب الأمن الرئيس - فريق ECAM - externalcyberassurance@barclayscorp.com)
• 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></table></td>
<td>إذا لم يتم تنفيذ هذا الضابط، فقد لا يتمكن المورّد من تقييم التهديدات السيبرانية التي يواجهها والوقوف على مدى ملاءمة دفاعاته وقوتها على التصدي لها.
قد يتم الكشف عن معلومات بنك باركليز و/أو قد يحدث فقدان للخدمة يسفر عن ضرر تنظيمي أو إضرار بالسمعة.</td>
</tr>
</table>

		P2	عالٍ	30	
		P3	متوسط	60	
		P4	منخفض	180	
		P5	معلوماتي	360	
16. 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. يجب أن يقوم المورد بسحب مفاتيحه بعد انتهاء فترة الخدمة أو إعداد برنامج إلزامي لتناوب المفاتيح. • 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 وقترة 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. ○ 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: ○ في حدود التشفير لجهاز صلب/وحدة أمن صلبة معتمدة. ○ في شكل مشفر بموجب مفتاح قائم آخر أو مشتق من كلمة المرور. ○ في أجزاء مكونات منقسمة، ومقسمة بين مجموعات حفظ منفصلة. ○ المسح في ذاكرة المضيف طوال فترة عملية التشفير، ما لم تكن مطلوبة في حماية وحدة أمن الأجهزة (HSM). • يجب على المورّد التأكُّد 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.	تضمن حماية التشفير وخوارزمياته المحدَّثة والمناسبة حماية مستمرة لأصول معلومات بنك باركليز.

	○ المفاتيح التي تحمي المستودعات المجمَّعة والمخزّنة 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 وحماية 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 المورّد توافق الخوارزميات وطول المفاتيح المستخدمة مع المعهد الوطني للمعايير والتكنولوجيا (NIST) وأفضل ممارسة في الصناعة.	
17. الحوسبة السحابية	يجب على المورّد (عميل خدمة السحابة (CSC)) التأكُّد من ضرورة وجود إطار عمل محدَّد جيدًا للضوابط الأمنية في خدمة السحابة المستخدمة للخدمة (الخدمات) المقدَّمة إلى بنك باركليز، وذلك لتحقيق أهداف السريَّة والنزاهة والتوافر ولضمان وجود الضوابط الأمنية وعملها بفاعلية لحماية الخدمة (الخدمات) المقدَّمة إلى بنك باركليز. ينبغي اعتماد المورّد 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.	إذا لم يتم تنفيذ هذا الضابط الخاص بالسحابة، فقد تكون بيانات بنك باركليز عرضة للخطر، ما قد يؤدي إلى ضرر تنظيمي أو إضرار بالسمعة.

	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. يجب أن يطلب المورّد دليلاً موثَّقًا على أن تطبيق ضوابط أمن المعلومات وإرشاداتها المتعلقة بخدمة السحابة يتماشى مع أي ادعاءات يقدمها مقدم خدمة السحابة. تقع على عاتق المورّد مسؤولية التأكُّد من أنَّ الضوابط الأمنية للبيانات المتعلقة بأصول معلومات/بيانات بنك باركليز، بما في ذلك المعلومات الشخصية داخل السحابة ومقدم خدمة السحابة، مسؤولة عن بيئة الحوسبة السحابية. يظل المورّد مسؤولاً عن تكوين تنفيذ الضوابط الأمنية ومراقبته للحماية من أي حوادث أمنية، بما في ذلك انتهاكات البيانات. يجب على المورّد 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) • حذف البيانات/مسح البيانات بشكل آمن • التشفير والترميز وإدارة المفتاح - CEK • التسجيل والمراقبة • الوضع الظاهري • الفصل بين الخدمات تجب مواقة بنك باركليز (مكتب الأمن الرئيس - فريق ECAM) على أصول معلومات/بيانات بنك باركليز، بما في ذلك المعلومات الشخصية المُخزَّنة في السحابة كجزء من الخدمة المُقدَّمة إلى بنك باركليز. يجب على المُورّد تزويد بنك باركليز بمواقع مناطق البيانات ومناطق بيانات تجاوز الفشل حيث سيتم تخزين بيانات بنك باركليز أو الاحتفاظ بها. يجب أن يؤكد المُورّد أدوار أمن المعلومات ومسؤولياته المرتبطة بخدمة السحابة، وذلك على النحو الموضح في اتفاقية الخدمة. ويمكن أن تشمل هذه الإجراءات العمليات التالية: • الحماية من البرامج الضارة؛ • النسخ الاحتياطي؛ • ضوابط التشفير؛ • إدارة نقاط الضعف؛ • إدارة الحوادث؛ • اختبار الأمان؛ • التدقيق؛ • جمع الأدلة وصيانتها وحمايتها، بما في ذلك السجلات وسجلات التدقيق؛ • حماية المعلومات عند إنهاء اتفاق الخدمة؛	

	• إدارة الهوية والوصول.	
18. 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). 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 الأساسية لتكنولوجيا المعلومات بالكامل بواسطة **المورّد** وتتصل ببوابات الشبكة الخارجية لـ **بنك باركليز** - يمتلك المورّد أجهزة الشبكة المحلية والشبكة اللاسلكية وسطح المكتب ويديرها. المستوى 3 (الدرجة الاقتصادية) - تتم إدارة البنية التحتية لتكنولوجيا المعلومات بالكامل بواسطة **المورّد** وتتصل ببوابات الإنترنت من **بنك باركليز** - يمتلك المُورّد أجهزة LAN وWAN وسطح المكتب ويديرها.	إذا لم يتم تنفيذ هذا الضابط، فقد لا يتم وضع الضوابط المادية والتقنية المناسبة، ما يؤدي إلى تأخير الخدمة أو تعطيلها أو حدوث انتهاكات أمنية سيبرانية/حوادث أمنية.
18.1 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.	
18.2 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. • يجب تقييد الدخول إلى مناطق BDS والخروج منها ومراقبتها من خلال آليات التحكم في الوصول المادي لضمان عدم السماح لغير الموظفين المصرّح لهم بالوصول. • 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 والموظف غير الظاهر (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: بالنسبة إلى الموظف المصرّح له: ○ شارة هوية تحمل صورة مرئية طوال الوقت ○ يتم تطبيق قارئات البطاقات التي تعمل بالتقريب ○ يتم تمكين آلية المرور مرة واحدة فقط ومراقبتها • يلزم أن يتبنى المورد عمليات وإجراءات للتحكم في الأشخاص الخارجيين ومراقبتهم، بما في ذلك المتعهدون من الباطن وجهات معالجة البيانات من الباطن التي لديها إمكانية الوصول المادي إلى مناطق BDS لأغراض الصيانة وعمال النظافة.	
18.3 BDS - المراقبة بالفيديو	• تنفيذ مراقبة مساحة BDS بالفيديو للكشف الفعال عن الوصول غير المصرح به و/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.	

18.4 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 - 4 العمل عن بُعد (الوصول عن بُعد)
18.5 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).
18.6 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 منطقيًّا بين شبكة BDS وشبكة شركة المورّد باستخدام جدار الحماية، ويجب تقييد حركة مرور البيانات 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؛ o 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 - 2 أمن الحدود والشبكات
18.7 المساحة المخصصة للبنك – الشبكة اللاسلكية	تعطيل الشبكة اللاسلكية لتوفير شبكة BDS لخدمات بنك باركليز.
18.8 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 القرص الصلب بالكامل؛ • تعطيل جميع البرامج/الخدمات/المنافذ غير المطلوبة؛ • تعطيل الوصول إلى حقوق الإدارة للمستخدم المحلي؛ • لن يتم السماح للموظف التابع للمورّد بتغيير الإعدادات الأساسية مثل: حزمة الخدمة الافتراضية والخدمات الافتراضية وما إلى ذلك؛ • تعطيل منفذ USB المستخدم لنسخ معلومات/بيانات بنك باركليز إلى وسائط خارجية • التحديث باستخدام أحدث توقيعات مكافحة البرمجيات الضارة وتصحيحات الأمان؛ • تقييد منع فقدان البيانات بعدم استخدام القص والنسخ واللصق وطباعة الشاشة أو أداة الالتقاط مع بيانات بنك باركليز؛

	• يجب تعطيل خيار "تعطيل الوصول إلى الطابعة" بشكل اقتراضي • ينبغي تعطيل مشاركة/نقل أصول معلومات/بيانات بنك باركليز باستخدام أدوات/برامج المراسلة الفورية؛ • الكشف عن حالة وجود و/أو استخدام برامج غير مصرح بها، بما في ذلك البرامج الضارة، وإيقافها ومعالجتها. الرجوع إلى المراقبة - 8 أمن نقطة النهاية	
18.9 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.	
18.10 - BDS BYOD/الجهاز الشخصي	**يلزم عدم السماح للأجهزة الشخصية/BYOD بالوصول إلى بيئة بنك باركليز و/أو بياناته**	
حق الفحص	يجب 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 و/أو المتعهدون معه من الباطن لتطوير أنظمة المورد المستخدمة في الخدمات أو اختبارها أو تعزيزها أو صيانتها أو تشغيلها، من أجل مراجعة امتثال المورد لالتزاماته. يجب على المورّد كذلك السماح لبنك باركليز بإجراء الفحص كل عام على الأقل و/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 المورّد 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 متعهدين من الباطن أو جهات معالجة بيانات 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).
المعلومات 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.
الجهاز الظاهري:	البيئة الكاملة التي تدعم تنفيذ برنامج الضيف. ملحوظة – الجهاز الظاهري هو تضمين كامل للأجهزة الظاهرية والأقراص الظاهرية وبيانات التعريف المرتبطة بهما. تسمح الأجهزة الظاهرية بالإرسال المتعدد عبر الأجهزة المادية الأساسية من خلال طبقة برامج تسمى مراقب الأجهزة الافتراضية.

السرية البنكية

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

مجال/عنوان الرقابة	وصف الضابط	سبب الأهمية
1. الأدوار والمسؤوليات	يجب على المورّد تحديد الأدوار والمسؤوليات والمساءلات ومشاركتها فيما يتعلق بالتعامل مع البيانات المحدِّدة لهوية العميل (يشار إليها فيما يأتي بالاختصار CID). تجب على المورّد مراجعة الوثائق التي تسلِّط الضوء على الأدوار والمسؤوليات والمساءلات الخاصة بالبيانات المحدِّدة 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 المحدِّدة 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 المحدِّدة 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 المحدِّدة 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 المطبقة 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	يجب 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. يجب على المورّد 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 قيامهم باستيعاب مسؤولياتهم في ما 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 كل استخدامات الحوسبة السحابية و/أو التخزين الخارجي للبيانات المحدّدة لهوية العميل (في الخوادم خارج نطاق دائرة اختصاص السرية البنكية أو خارج البنية الأساسية للمورّد) المستخدمة كجزء من الخدمة المقدمة إلى دائرة الاختصاص هذه من قِبل الفرق المحلية ذات الصلة (ومن بينها مكتب الأمن الرئيس، الامتثال والقانون)، ويجب تنفيذ الضوابط وفقَ القوانين واللوائح المعمول بها في دائرة اختصاص السريَّة البنكية المطابقة من أجل حماية معلومات البيانات المحدّدة لهوية العميل في ما يتعلق بملف التعريف العالي الأخطار الذي يقدمونه.	إذا لم يتم تنفيذ هذا المبدأ، فقد تكون بيانات العميل المحمية (البيانات المحدّدة لهوية العميل) على نحو غير ملائم عرضة للخطر، ما قد يؤدي إلى فرض عقوبات قانونية وتنظيمية، أو إضرار بالسمعة.

الملحق B: 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
الموظف التابع للمورد	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 من دون امتيازات تصاعدية.

الملحق C: 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 ـ 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// العميل المتوقع	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

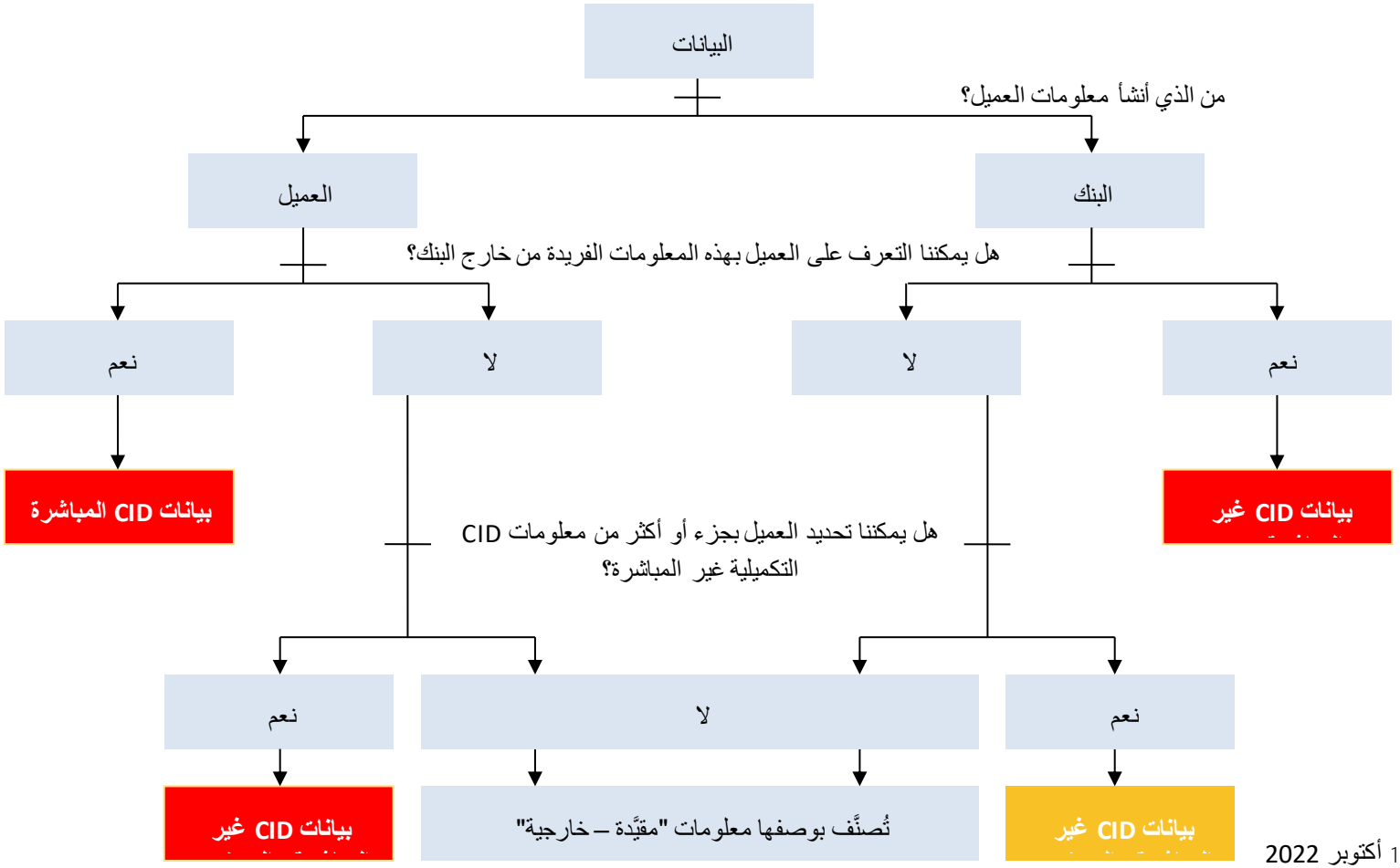
(= DCID) انتهاك السرية البنكية

2. معرف هوية الحاوية

(= L1 DCID) انتهاك السرية البنكية

3. حالة الثروة + الجنسية

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



الملحق D: مخطط التسميات المعلوماتية لبنك باركليز

الجدول D1: 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 مباشرة. 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 وقد 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 ومعلوماتهم الشخصية.

	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.	• تقييم مدى التأثر. • نتائج التدقيق والتقارير.
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 D2: **مخطط التسميات المعلوماتية - متطلبات المعالجة**

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

مرحلة دورة الحياة	متطلبات السرية البنكية
الإنشاء والتسمية	وفق "مقيّدة 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 "مقيَّدة 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 "مقيَّدة 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 تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من 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 تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من 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 تقتصر وسيلة توزيع الأصول على استخدام الأنظمة أو الأساليب أو المورّدين المعتمدين من 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.