التزام مراقبة المورّد الخارجي

الأمان المادي

الإصدار 10.0، بتاريخ أكتوبر 2020

نطاق الرقابة	وصف الرقابة	الأهمية
1. تقييمات المخاطر الأمنية	سيضمن الموردون إجراء تقييمات المخاطر الأمنية لمراجعة تدابير الأمان المادي وعملياته. ويجب أن يستكمل التقييمات شخص ذو خبرة أو مؤهل مناسبين مع مراعاة مدى ملاءمة ضوابط الأمان المادي وفعاليته للتخفيف من حدة كل من ملف المخاطر الحالي للمبنى وأي مشكلات ناشئة قد تؤثر في الموقع. ويتعين أن يكون معدل تكرار إجراء تقييم المخاطر متوافقًا مع الغرض من الموقع وأهميته. ومن المتوقع أن يتم تقييم المواقع المهمة لتشغيل عمليات بنك باركليز (متضمنة مراكز البيانات) مرة كل سنة على الأقل. يلزم توثيق نتائج تقييم المخاطر الأمنية، ووضع خطط عمل، وتعيين مسؤول للمشكلات/المخاطر المحددة وتتبعها حتى يتم الوصول لنتيجة. ويجب إخطار بنك باركليز بكل النتائج المهمة في غضون 10 أيام عمل من اكتشافها.	تُعد تقييمات المخاطر الأمنية مطلبًا أساسيًا لتقديم تقييم دقيق لبيئة الأمان المادي الخاصة بالمورد والضوابط والعمليات ومدى فعاليتها الحالية. وستحدد مواطن الضعف وفجوات الرقابة الجديدة أو الحالية وتقلل من أخطار الخسائر أو الأضرار التي تلحق بأصول بنك باركليز والإضرار بالسمعة المصاحبة و/أو فرض غرامة أو إدانة تنظيمية.
2. التحكم في الوصول	يتعين استخدام التحكم في الوصول الإلكتروني أو الميكانيكي أو الرقمي وإدارته في كل أماكن العمل التي تضطلع بالأنشطة المتعلقة بعقود بنك باركليز. وينبغي كذلك تثبيت كل أنظمة الأمان وتشغيلها وصيانتها وفق المتطلبات القانونية والتنظيمية. يجب أن يقتصر الوصول إلى النظام على الموظفين المصرح لهم بذلك، وتلزم إدارة الوصول إلى المفاتيح والتركيبات والتحكم فيها بدقة. تتعين إدارة كل بيانات اعتماد الوصول بفعالية للحد من مخاطر الوصول غير المصرح به. وتنبغي إدارة بيانات اعتماد الوصول بما يتماشى مع إجراءات التحكم في الوصول الخاصة بالمورد. وتصدر بيانات اعتماد الوصول عند تلقي الموافقة المناسبة. وتلزم إعادة التصديق على كل وسائل الوصول إلى المناطق المقيدة على فترات زمنية مناسبة. وإذا لم يعد الوصول إلى أماكن أو مناطق مقيدة مطلوبًا، فيجب إلغاء تنشيط بيانات اعتماد الوصول في غضون 24 ساعة من الإخطار.	يشكل التحكم الفعّال في الوصول جزءًا من الضوابط متعددة المستويات المطلوبة لحماية أماكن العمل من الوصول غير المصرح به وضمان أمان الأصول. وما لم يتم اتخاذ تدابير فعّالة للتحكم في الوصول، فثمة مخاطر من أن الموظفين غير المصرح لهم يمكنهم الدخول إلى مواقع الموردين أو المناطق المقيدة داخل مواقعهم. وقد يؤدي هذا إلى زيادة مخاطر الخسارة أو الأضرار التي تلحق بأصول بنك باركليز، وقد تتسبب في خسائر مالية وإضرار بالسمعة المصاحبة و/أو فرض غرامة أو إدانة تنظيمية.

3. أنظمة كشف المتسللين وكاميرات المراقبة	يتعين نشر أنظمة كشف المتسللين (IDS) وكاميرات المراقبة لمنع طرق الوصول غير المناسبة أو الأنشطة الإجرامية وكشفها ومراقبتها وتحديدها. ويجب نشر التجهيزات بما يتناسب مع تهديدات الأمان المادي السائدة التي تم تحديدها في أثناء نشاط تقييم المخاطر الأمنية لكل موقع. ويتعين تركيب كل أنظمة الكاميرات وأنظمة كشف المتسللين وتشغيلها وصيانتها وفق معايير الصناعة المقبولة. ويجب أن يقتصر الوصول إلى النظام على الموظفين المصرح لهم بذلك.	تشكل أنظمة كشف المتسللين وأنظمة كاميرات المراقبة جزءًا من الضوابط متعددة المستويات لحماية أماكن العمل من الوصول غير المصرح به، وضمان أمن الأصول. وما لم يتم تركيب هذه الأنظمة وتشغيلها وصيانتها بشكل فعّال، فثمة مخاطر من الوصول غير المصرح به إلى المواقع والمباني التي تحتوي على أصول بنك باركليز وبياناته، وبالتالي لن يتم الكشف عن الوصول غير المصرح به في الوقت المناسب.
4. أفراد الأمن	يجب نشر أفراد الأمن بما يتناسب مع التهديد الأمني المادي السائد في كل موقع. يلزم إشراك كل أفراد الأمن (سواء أكانوا موظفين لدى المورد أم المالك أم المورد الخارجي) أو التعاقد معهم من خلال مقدم خدمة معتمد ومرخص وفق التشريعات المحلية. وينبغي أن يتلقى الأفراد تدريبًا أمنيًا بما يتناسب مع دورهم ومسؤولياتهم. كما يلزم توثيق جميع التدريبات المقدمة والاحتفاظ بسجل تدريبي لكل أفراد الأمن.	يشكل أفراد الأمن جزءًا من الضوابط متعددة المستويات لحماية أماكن العمل من الوصول غير المصرح به وضمان أمن الأصول. وما لم يتم نشر أفراد الأمن بما يتماشى مع التهديد الأمني السائد وتدريبهم بشكل مناسب، فقد يحدث الوصول غير المصرح به إلى المواقع والمباني التي تحتوي على أصول بنك باركليز وبياناته، أو قد لا يتم الكشف عنه في الوقت المناسب. وقد يؤدي هذا إلى زيادة مخاطر الخسارة أو الأضرار التي تلحق بأصول بنك باركليز، وقد تتسبب في خسائر مالية وإضرار بالسمعة المصاحبة و/أو فرض غرامة أو إدانة تنظيمية.
5. إدارة الحوادث الأمنية ومستويات الاستجابة لها	سيطبق الموردون إجراءات لإدارة الحوادث الأمنية وإجراء التحقيقات عند الاقتضاء. وإذا تأثرت أصول بنك باركليز بالحادث، فلا بد من إبلاغ بنك باركليز بذلك في غضون 48 ساعة ومشاركة التقارير الرسمية وتفاصيل التحقيقات في أقرب وقت ممكن عمليًا، على ألا يتجاوز ذلك 10 أيام عمل بعد هذا الحادث. وهذا يتضمن بيانات التحكم في الوصول وصور كاميرات المراقبة عند الاقتضاء، بما يتماشى مع القوانين واللوائح المحلية.	إذا لم يتم تنفيذ هذا المطلب، فقد لا يتمكن بنك باركليز من الوثوق في أن المورد لديه إجراءات موثقة بصورة ملائمة لإدارة الحوادث الأمنية. وقد يؤدي ذلك إلى اتخاذ إجراء غير مناسب في أعقاب حادث ما، وهذا ما يزيد من مخاطر الخسائر أو الأضرار التي تلحق بأصول بنك باركليز أو بياناته وإضرار بالسمعة المصاحبة و/أو فرض غرامة/إدانة تنظيمية.
6. النقل	سيضمن الموردون نقل كل أصول بنك باركليز وبياناته بشكل آمن مع فرض ضوابط تتناسب مع قيمة الأصول والبيانات التي يتم نقلها (سواء من منظور الضرر المالي أو الإضرار بالسمعة)، وبيئة التهديد التي يتم النقل فيها.	لحماية أصول بنك باركليز أو بياناته في أثناء النقل بين مواقع المورد و/أو مواقع بنك باركليز، وهذا ما يقلل من مخاطر الخسارة أو السرقة أو الضرر والإضرار بالسمعة المصاحبة و/أو فرض غرامة/إدانة تنظيمية.

7. المراكز والقاعات الخاصة بالبيانات	يتم تأمين كل مراكز البيانات ومقدمي الخدمات السحابية وقاعات البيانات المستقلة والموجودة في مواقع مشتركة والتابعة لجهات خارجية بشكل فعّال لمنع الوصول غير المصرح به والسرقة أو الإضرار بأصول بنك باركليز أو بياناته. ويلزم أن تكون كل مراكز البيانات لديها ضوابط تقنية ومادية وبشرية متعددة المستويات وإجراءات خاصة بالموقع لحماية محيط قاعات البيانات وبنائها وسلامتها بشكل فعال. وتشمل الضوابط -على سبيل المثال لا الحصر- كاميرات المراقبة وأنظمة كشف المتسللين والتحكم في الوصول.	لحماية أصول بنك باركليز أو بياناته المحفوظة داخل مراكز البيانات وقاعات البيانات والمواقع ذات الأهمية المماثلة من مخاطر الخسارة أو التلف أو السرقة الناجمة عن الوصول غير المصرح به إلى الأماكن المقيدة.