الخارجيين المورّدين مراقبة التزامات

الأمن المادي (الضوابط الفنية)

الإصدار 12.0، أكتوبر 2022

عنوان الضابط	وصف الضابط	سبب الأهمية
1. التحكم في الوصول (TC 5.1)	يجب استخدام التحكم في الوصول الإلكتروني أو الميكانيكي أو الرقمي وإدارته في كل المرافق التي تضطلع بالأنشطة المتعلقة بعقود بنك باركليز. وينبغي كذلك تثبيت كل أنظمة الأمان وتشغيلها وصيانتها وفق المتطلبات القانونية والتنظيمية. يجب أن يقتصر الوصول المنطقي والإداري إلى أنظمة التحكم في الوصول الإلكتروني على الموظفين المصرّح لهم وتجب إدارة الوصول إلى المفاتيح والتوليفات المادية والتحكم فيها بصرامة. يجب الاحتفاظ بسجل تدقيق يضم حاملي بيانات الاعتماد/المفاتيح/التوليفات، بما يشمل منح أذونات الوصول وتعديلها وإلغاءها. تجب إدارة كل بيانات اعتماد الوصول بفعالية للحد من مخاطر الوصول غير المصرح به. وتجب إدارة بيانات اعتماد الوصول بما يتماشى مع إجراءات التحكم في الوصول الخاصة بالمورّد. يمكن إصدار بيانات اعتماد الوصول عند تلقي الموافقة المناسبة. تجب إعادة التصديق على كل إمكانات الوصول إلى المناطق المقيدة على فترات زمنية مناسبة. إذا لم تعُد هناك حاجة للوصول إلى مبنى أو منطقة محظورة، يجب إلغاء تنشيط بيانات اعتماد الوصول بواسطة القسم المسؤول عن إدارة بيانات اعتماد الوصول في غضون 24 ساعة من تلقي إشعار من وحدة الأعمال أو الإدارة ذات الصلة التي تقدم المشورة بشأن التغيير في متطلبات الموظف المعنيّ (على سبيل المثال، تغيير الدور أو المسؤوليات، أو الفصل من العمل أو التوظيف). إذا كان العمل عن بُعد مطلوبًا؛ حيث سيقوم المورّد أو المتعهدون من الباطن التابعون له بالوصول إلى معلومات بنك باركليز أو تخزينها أو معالجتها في صيغة مادية أو ظاهرية تكون مقيَّدة بطبيعتها (بما في ذلك البيانات الشخصية أو أي معلومات حسَّاسة مقدَّمة إلى المورّد بناءً على ضرورة معرفته للمعلومة)، يجب أن يوافق المورّد على هذه الترتيبات جنبًا إلى جنب مع بنك باركليز قبل الوصول إلى هذه البيانات.	يُعدُّ الحفاظ على فعالية نظام التحكم في الوصول وعمليات إدارة الوصول وإجراءاته مكونًا أساسيًا في مجموعة من الضوابط المفروضة على مستوى الطبقات اللازمة لحماية المنشآت من الوصول غير المصرّح به ولضمان أمن الأصول. وما لم يتمّ اتخاذ تدابير فعّالة للتحكم في الوصول، فثمة مخاطر من أن الموظفين غير المصرّح لهم يمكنهم الدخول إلى مواقع المورّدين أو المناطق المقيدة داخل مواقعهم. وقد يؤدي ذلك 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.
2. أنظمة كشف المتسللين وكاميرات المراقبة (TC 5.2)	يجب نشر أنظمة كشف المتسللين (IDS) وكاميرات المراقبة لمنع الوصول غير المشروع أو الأنشطة الإجرامية وكشفهما ومراقبتهما ورصدهما. يجب نشر المعدات بما يتناسب مع تهديدات الأمن المادي السائدة التي تم تحديدها في أثناء تقييمات مخاطر الأمن لكل موقع. يجب تركيب كل أنظمة الكاميرا وأنظمة كشف المتسللين (IDS) وتشغيلها وصيانتها وفقًا لمعايير الصناعة الحالية (على سبيل المثال، المنظمة الدولية للمعايير ((ISO، ومراقبة النظام والمؤسسة ((SOC، والمتطلبات القانونية والتنظيمية السائدة والمواصفات الحالية المقدمة من الجهات المصنّعة). يجب تطبيق الإجراءات لضمان مراقبة إنذارات أنظمة كشف المتسللين (IDS) وكاميرات الأمان وإدارتها بفاعلية. ويجب أن يقتصر الوصول إلى نظام الأمن على الموظفين المصرّح لهم بذلك.	تشكل أنظمة كشف المتسللين وأنظمة كاميرات المراقبة جزءًا من الضوابط المتعددة المستويات لحماية أماكن العمل من الوصول غير المصرّح به، وضمان أمن الأصول. وما لم يتم تركيب هذه الأنظمة وتشغيلها ومراقبتها وصيانتها بشكل فعّال، فثمة مخاطر من الوصول غير المصرّح به إلى المواقع والمباني التي تحتوي على أصول بنك باركليز وبياناته، ومن ثمّ لن يتم الكشف عن الوصول غير المصرح به في الوقت المناسب.

3. تركيبات مراكز البيانات، والقاعات الرئيسية، وأجهزة الاتصالات (TC 5.3)	يجب تأمين كل مراكز البيانات المستقلة والموجودة في مكان مشترك والتابعة لجهات خارجية ومقدمي خدمة السحابة وتركيبات قاعات البيانات وأجهزة الاتصالات (بما في ذلك غُرف الخوادم وغُرف الاتصالات المستقلة) بشكل فعّال لمنع الوصول غير المصرّح به إليها أو سرقة أصول بنك باركليز أو بياناته أو إلحاق الضرر بهما. ويجب أن تكون كل مراكز البيانات لديها ضوابط تقنية ومادية وبشرية متعددة المستويات وإجراءات خاصة بالموقع لحماية محيط قاعات البيانات وجميع المناطق الحيوية الأخرى وبنائها وسلامتها بفاعلية. وتشمل الضوابط، على سبيل المثال لا الحصر، كاميرات المراقبة وأنظمة كشف المتسللين والتحكم في الوصول وموظفي الأمن. عندما تكون عمليات التركيب في مواقع مشتركة، يجب نشر أمان فعّال حول إمكانات عزلها المستقلة.	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 المصرّح به إلى الأماكن المقيّدة.

تجب قراءة هذا المعيار مع المعيار التالي، حيث يجب تطبيق الضوابط الإدارية المحددة باعتبارها ضمن النطاق:

التزام مراقبة مقدم الخدمة الخارجي ((TPSPCO، متطلبات التحكم في الإدارة - أمن المعلومات، والأمن الإلكتروني والمادي، والتكنولوجيا، وتخطيط الاسترداد، وخصوصية البيانات، وإدارة البيانات، وPCI DSS وضوابط EUDA.