التزامات مراقبة المورّدين الخارجيين

الأمن المادي (الضوابط الفنية)

الإصدار 14.0، بتاريخ أكتوبر 2024

عنوان الضابط	وصف الضابط	سبب الأهمية
1. التحكم في الوصول (TC 5.1)	يجب تحديد قواعد مراقبة الوصول لجميع المناطق الآمنة، المدعومة بالإجراءات الرسمية المعتمدة والمسؤوليات المحددة. يجب حماية المناطق الآمنة بواسطة عناصر التحكم في الدخول ونقاط الوصول المناسبة باستخدام التحكم الإلكتروني أو الميكانيكي أو الرقمي. 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 الفريدة عند تلقي الموافقة المناسبة. تجب إعادة بيانات 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).	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. أمن المحيط والمباني والمساحة (TC 5.2)	يجب تحديد محيط الأمن وتنفيذه لحماية المناطق التي تحتوي على معلومات وغيرها من الأصول المرتبطة، بما يتناسب مع بيئة المخاطر والمخاطر المحددة والمتوقعة. الأمن المادي للمكاتب، والغرف، ويجب تصميم المرافق (بما في ذلك أنظمة التحكم في الوصول وكاميرات الأمان وأنظمة الكشف عن الدخلاء وغيرها من الضوابط التقنية المناسبة) وتنفيذها على أساس نهج قائم على المخاطر يستند إلى مستويات التهديد الحالية والمتوقعة، كما يجب أن تكون متناسبة مع عمليات الأعمال التي تتم وقيمة المعلومات والأصول. ويجب تصميم وتنفيذ العمليات الأمنية للعمل في المناطق الآمنة. يجب تحديد قواعد المكتب الواضحة للأوراق ووسائط التخزين القابلة للإزالة وقواعد الشاشة الواضحة لمرافق معالجة المعلومات وتطبيقها بشكل مناسب. 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. عندما تكون التركيبات في مواقع مشتركة، يجب نشر ضوابط أمنية فعالة لتفعيل الفصل والمراقبة المنفصلين	لحماية أصول باركليز أو البيانات الموجودة داخل مراكز البيانات وقاعات البيانات ومباني الموردين (التي يحتفظ بها المورد والطرف الثالث على حد سواء) من مخاطر الخسارة أو التلف أو السرقة الناتجة عن الوصول غير المصرح به إلى مساحة محدودة.

3. الحماية من التهديدات المادية للبنية التحتية والأصول (TC 5.3)	يجب تصميم الحماية من التهديدات المادية للبنية التحتية والأصول وتنفيذها من خلال نشر كاميرات الأمن وأنظمة اكتشاف الدخلاء و/أو غيرها من الضوابط الأمنية ذات الطبقات المناسبة لبيئة التهديدات السائدة والمتوقعة. يجب مراقبة المباني باستمرار لضمان الوصول المادي غير المصرح به. يجب ربط المعدات بإحكام وحمايتها. يجب حماية الكابلات التي تنقل الطاقة أو البيانات أو خدمات المعلومات الداعمة من الاعتراض المادي أو التداخل أو التلف. يجب تركيب معدات الأمان والتركيبات وصيانتها وفقًا لمتطلبات الجهة المصنعة ومراقبتها لضمان توفر المعلومات وسلامتها وسريتها. يجب حماية أصول باركليز التي يتم الاحتفاظ بها خارج الموقع أثناء الراحة وأثناء النقل. يجب تركيب المعدات وصيانتها بشكل صحيح ووفقًا لمعايير الصناعة السائدة لضمان توفر المعلومات وسلامتها وسريتها. يجب أن يتوافق تركيب جميع أنظمة الأمان وتشغيلها مع المتطلبات القانونية والتنظيمية السائدة. حيثما وجدت، يجب التحكم في مناطق التسليم والتحميل بشكل مناسب وعزلها عن المرافق التشغيلية لتجنب الوصول غير المصرح به والتهديد المحتمل الناتج عن عمليات التسليم التي لم يتم التحقق منها.	سيؤدي نشر ضوابط أمان مادية وتشغيلها بما يتناسب مع التهديدات الحالية والمتوقعة إلى الحد من تأثير الوصول غير المصرح به أو السرقة أو التلف المتعمد للمباني والأصول أو منعه.

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.