متطلبات CITI للمورّدين

المالك:
رئيس التعهيد العالمي في Citi

تاريخ الإصدار:
يناير ٢٠١٥

تاريخ المراجعة:
مارس 2022

الإصدار:
6.0

جدول المحتويات

1 لمحة عامة

1.1 المتطلبات بشكل عام

توضح متطلبات Citi للمورّدين (يُشار إليها باسم **"المتطلبات"**) التي بين أيدينا بعض الالتزامات التي يجب على المورّدين الوفاء بها أثناء ممارسة الأعمال التجارية مع Citi. تسري بعض المتطلبات على جميع المورّدين، بينما يعتمد تطبيق المتطلبات الأخرى على مورد معين على أنواع المنتج (المنتجات) والخدمة (الخدمات) التي يقدمها ذلك المورّد إلى Citi (تم تلخيص تلك المتطلبات الأخيرة في القسم 1-2 أدناه وترد الإشارة إليه في بداية كل حكم مذكور فيها). يكون للمصطلحات الواردة المعاني المقابلة لكل منها طي هذه الاتفاقية، بما في ذلك الملحق المرفق، ما لم يتم الإشارة إلى ذلك المعنى طيه، وفي هذه الحالة يكون لتلك المصطلحات المعنى المحدد لها في العقد، على النحو المعرّف أدناه.

هذه المتطلبات عبارة عن التزامات تعاقدية بموجب اتفاقيات المورّد مع Citi (بما في ذلك، على سبيل المثال لا الحصر، وثائق المعاملات، مثل أوامر العمل وجداول الترخيص) (يُشار إلى كلٍ منها باسم **"عقد"**)، بالإضافة إلى أي التزامات محددة في أي اتفاقية، أو أي التزامات بموجب القانون المعمول به (كما هو معرّف أدناه)، أو أي إشعار يُقدم للمورد من Citi لإبلاغ المورّد بالتزاماته بموجب نفس القانون (يُشار إلى كلٍ منها باسم **"إشعار"**)، أو أي متطلبات إضافية تكون أكثر تحديدًا تنفذها أعمال أو وظائف Citi. هذا وسوف تسري الالتزامات والمتطلبات الأكثر صرامة فيما يتصل بأي تعارض بين أي من المتطلبات السابقة والقيود. يجب على المورّدين القيام بدور استباقي والتشاور مع جهة الاتصال الرئيسية للأعمال في Citi (أو من ينوب عنها) فيما يتعلق بأي أسئلة لديهم بخصوص هذه المتطلبات، بما في ذلك أي تغييرات يتم إدخالها عليها، أو أي إعفاء يتم طلبه منها، أو أي تعارض محتمل فيها أو مع القانون المعمول به.

يجوز أن يترتب على عدم الامتثال لهذه المتطلبات أو أي متطلبات إضافية تحددها شركة تابعة لـ Citi والتي يتعامل معها المورّد إنهاء عقد المورّد مع Citi. علاوة على ذلك، يمكن أن تُعتبر انتهاكات المتطلبات أيضًا انتهاكات للقانون المعمول به وقد تؤدي إلى نشوء تعويضات عن أضرار مدنية تُستحق إلى Citi (أو أطراف ثالثة) أو عقوبات جنائية على المورّد. لا يجوز للمورّدين استخدام الامتثال لسياساتهم الخاصة كبديل لالتزامهم بالامتثال لأي من أحكام هذه المتطلبات دون موافقة كتابية من Citi.

2.1 المتطلبات المطبقة على بعض المورّدين الانتقائيين

يوضح الجدول التالي بعض المتطلبات التي تنطبق على بعض المورّدين الذين يستوفون معايير التطبيق المحددة في تلك المتطلبات. الأقسام غير المذكورة أدناه تنطبق على جميع المورّدين.

رقم القسم	عنوان القسم	قابلية التطبيق
12	مكافحة غسل الأموال	تسري على المورّدين الذين يؤدون خدمات معينة تتعلق بالعملاء (مثل الالتحاق بالخدمة وحساب العميل وفحص المعاملة) أو تسليم البيانات / المقاييس المتعلقة بالأنشطة السابقة؛ و/أو المورّدين الذين يعملون كوسيط فيما يتعلق بالنقد أو الأدوات المالية (مثل خدمات استقبال الإيداع عن بعد أو البريد السريع أو سيارات نقل الأموال المصفحة أو الخزائن المصفحة).
13	إدارة السجلات	تسري على المورّدين الذين يقومون بالوصول إلى معلومات Citi ومعالجتها وتخزينها
14	خدمات التعامل مع العملاء	تسري على تعاملات المورّد مع أي فرد بصفته عميلاً سابقًا أو حاليًا أو محتملًا لـ Citi أو لطرف ذي صلة (كموظف أو ممثل) لهذا العميل (يُشار إلى كل فرد من هؤلاء باسم "العميل").
15	استمرارية الأعمال	تسري على المورّدين المدرجين في خطة التعافي لوحدة أعمال Citi أو إذا كان المورّد يستضيف تطبيقًا له إمكانات التعافي (مثل القدرة على استعادة التكنولوجيا الرقمية (TRTC))، والتي تستخدمها Citi. يتحمل مسؤول النشاط التجاري (BAO) مسؤولية توضيح قابلية التطبيق ومتطلبات استمرارية الأعمال (COB) للمورّد.
16	المعايير العالمية لفحص الخلفية الأمنية	تنطبق على المورّدين الذين يتمتع موظفوهم بإمكانية الوصول إلى أنظمة / شبكات Citi؛ و/أو الوصول دون مرافقة إلى مباني Citi (سيطلب من هؤلاء الأفراد أن يكون لديهم رقم تعريف الموظف العالمي (GEID)، وأن يكونوا مسجلين في إدارة لغير موظفي Citi؛ و/أو المورّدين الذين يمكنهم الوصول إلى/معالجة/تخزين/إدارة معلومات Citi السرية أو الأعلى
17	النفقات	تسري على المورّدين المؤهلين حسب العقود الموقعة معهم للمطالبة بنفقات أعمال قابلة للسداد
18	أمان المعلومات (IS)	يسري على المورّدين الذين يصلون إلى معلومات Citi أو يعالجونها أو يديرونها أو يخزنونها؛ و/أو المورّدين المسؤولين بصفتهم مضيفين لتطبيقات الإنترنت التي تحمل علامة Citi التجارية؛ و/أو المورّدين الذين لديهم اتصال بموارد شبكة Citi؛ و/أو المورّدين الذين يحتاجون وصول دون مرافقة إلى مرافق Citi
19	المبادئ التوجيهية لمكان العمل الآمن	
20	الذكاء الاصطناعي/التعلم الآلي	يسري على المورّدين الذين يستخدمون الذكاء الاصطناعي / التعلم الآلي (AI / ML)، على النحو المحدد من قبل Citi في أي جزء من المنتج/الخدمة التي يقدمونها.

2 تكافؤ فرص العمل / العمل الإيجابي

كجزء من جهودنا المبذولة للامتثال للمتطلبات التنظيمية الفيدرالية فيما يتصل بعدم التمييز والإجراءات الإيجابية، فقد وضعت شركة Citi برنامجًا وسياسات بشأن تكافؤ فرص العمل والعمل الإيجابي حيث صُممت خصيصًا لضمان تكافؤ فرص العمل لكل الأشخاص المؤهلين دون النظر إلى عرق أو لون أو دين أو جنس أو توجه جنسي أو هوية جنسية أو أصل قومي أو عمر أو حالة اجتماعية أو معلومات جينية أو إعاقة أو حالة المحاربين القدامة المكفولة أو أي سبب آخر محظور قانونًا.

ويتضمن ذلك، على سبيل المثال لا الحصر، ما يلي:

أ. التعيين أو التوظيف أو النقل أو إنزال الدرجة الوظيفية أو الترقية
ب. التوظيف أو الإعلان أو طلب التوظيف
ج. المعاملة أثناء فترة التوظيف
د. معدلات الأجور أو أشكال التعويض الأخرى
ه. الانتقاء للالتحاق بتدريب، بما في ذلك التدريب المهني
و. التسريح أو إنهاء العمل

يجب على المورّدين الامتثال، ومطالبة موظفيهم بالامتثال، لمتطلبات جميع قوانين ولوائح عدم التمييز والعمل الإيجابي المعمول بها، بما في ذلك، على سبيل المثال لا الحصر، أي من تلك القوانين أو اللوائح التي تخطر Citi المورّد بشأنها كتابيًا بأنه يجب عليه الامتثال لها.

ارجع إلى بيان سياسة العمل الإيجابي وتكافؤ فرص العمل في الولايات المتحدة من Citi للحصول على مزيد من المعلومات، والتي يمكن العثور عليها على الرابط https://www.ecfr.gov/current/title-41/subtitle-B/chapter-60/part-60-300#p-60-300.44(f)(1)(ii).

3 مكافحة الرشوة

تطبق Citi سياسات وإجراءات وضوابط داخلية للامتثال لقوانين مكافحة الرشوة وتحظر تمامًا الرشوة أو مدفوعات التسهيل بأي شكل من الأشكال. يجب على جميع موردي شركة Citi، أو أي شخص يعمل نيابةً عن شركة Citi، إنجاز أنشطتهم وفقًا لأعلى معايير السلوك المهني وهو ما يقتضي الامتثال لجميع القوانين التي تحظر أفعال الرشوة والفساد والاحتيال وتقديم بيانات زائفة، بما في ذلك القانون الأمريكي للممارسات الأجنبية الفاسدة ("FCPA")، والقانون البريطاني للرشوة، كل حسب التعديلات التي يتم إدخالها عليها، أو أي لوائح أو قوانين أو قواعد أخرى سارية فيما يتصل بمكافحة الرشوة أو مكافحة الفساد أو الاحتيال أو العمولات الخفية (يُشار إليها مجتمعة باسم "قوانين مكافحة الرشوة").

يلتزم أي مورد، وكذلك أي من موظفيه، الذين يعملون نيابةً عن Citi، بعدم القيام بما يلي: (1) دفع أو منح أو تقديم أي مدفوعات أو مزايا أو فوائد لأي شخص؛ أو (2) دفع أو منح أو تقديم أي مدفوعات أو مزايا أو فوائد لأي شخص؛ أو (3) تلقي أو قبول (سابقًا أو لاحقًا) أي مدفوعات أو مزايا أو فوائد أخرى من أي شخص، في كل حالة من حالات انتهاك مكافحة الرشوة. يتعين على المورّد إجراء أعماله نيابة عن Citi بما يتوافق مع هذه المتطلبات، بما في ذلك هذا القسم، حسب الاقتضاء. يجب على المورّدين كذلك وضع السياسات والإجراءات المناسبة لضمان امتثالهم لجميع قوانين مكافحة الرشوة.

للاطلاع على نظرة عامة حول برنامج مكافحة الرشوة الذي تطبقه Citi، يُرجى زيارة علاقات المستثمرين لدى Citigroup (تحت قسم "سياسات Citi" اختر "برنامج مكافحة الرشوة").

4 الهدايا والترفيه

لا يجوز للمورّدين تقديم الهدايا أو منح أي شيء ذي قيمة (بما في ذلك وسائل الترفيه) إلى موظفي Citi، إذ كان من شأن ذلك أن يؤدي إلى تضارب في المصالح بشكل فعلي أو ظاهري أو التأثير على نزاهة الموظف أو حُكمه، أو خلافًا لذلك التأثير على اتخاذ القرار من جانب الموظف بشكل غير سليم، أو اضطرار الموظف إلى التصرف بما يتعارض مع واجباته. ودون تقييد لما سبق، لا يُسمح بتقديم أي هدايا نقدية أو ما يعادلها بما في ذلك بطاقات الهدايا وشهادات الهدايا والمظاريف الحمراء (الهدايا التي تقدم في مناسبات اجتماعية) والقسائم تحت أي ظرف من الظروف، ويجب على المورّدين عدم تقديم هدايا تجارية غير نقدية تتجاوز في مجموعها ١٠٠ دولارًا أمريكيًا لكل شخص في السنة التقويمية إلى أي موظف من موظفي Citi. يخضع قبول أي موظف في شركة Citi لهدايا تجارية إلى الحصول على موافقة مسبقة وفقًا لمعيار الهدايا والترفيه لدى شركة Citi، وقد يخضع لقيود إضافية بموجب سياسات محددة لأعمال Citi و/أو سياسات الكيان الإقليمية و/أو القانونية.

وفي حال قيام المورّد بأنشطة ترفيهية مرتبطة بالأعمال (مثل دعوة لتناول وجبة طعام أو فعالية اجتماعية أو رياضية أو ثقافية أو أي من الفعاليات الأخرى المماثلة) لأي من موظفي Citi، يجب على المورّد حضور هذه الفعالية كما يجب أن تكون الأنشطة الترفيهية مناسبة ومعقولة أو مقبولة عرفًا وغير مبالغ فيها أو غير متكررة بشكل مفرط، وأن يكون واضحًا أنها لا تهدف إلى التأثير على أعمال Citi. إذا لم يكن المورّد حاضرًا في الفعالية، فسيتم اعتبار الترفيه بمثابة هدية عمل.

لا يجوز للمورّد، نيابة عن Citi أو بزعم أنه نيابة عنها، تقديم الهدايا أو الأنشطة الترفيهية أو أي شيء أيًا كانت قيمته إلى أي شخص خارج شركة Citi.

5 تنوع المورّدين ومبادئ المورّدين

نفذت Citi برنامج تنوع المورّدين والذي يشجع، من بين مبادرات أخرى، على استخدام الشركات المعتمدة بأنها مملوكة لأقليات أو نساء أو أفراد معاقين أو محاربين قدامى كمورّدين ومقاولين من الباطن (يشار إليهم باسم "موردون متنوعون") إلى أقصى حد ممكن لمساعدة المورّدين المتنوعين في نموهم وتطورهم على المدى الطويل. لمساعدة Citi في الامتثال لهذه الأهداف، يجب على المورّد، بما يتفق مع التزاماته الأخرى بموجب هذه الاتفاقية وإلى الحد الذي يستخدم فيه مقاولين من الباطن أو يشتري سلعًا أو خدمات فيما يتعلق بأداء المورّد لالتزاماته بموجب هذا العقد، بذل جهود بحسن نية لتخصيص ما لا يقل عن 15% من المبلغ الذي ينفقه المورّد فيما يتعلق بمقاوليه من الباطن لتوفير السلع والخدمات التي يتم الحصول عليها من مورّدين متنوعين. يقوم المورّد بتزويد Citi بالمعلومات المتعلقة بنفقات المورّد، سواء المباشرة أو غير المباشرة، مع المورّدين المتنوعين من خلال استكمال "نموذج ملف تعريف التنوع المستوى 2" (والذي يمكن أن توفره Citi على أساس ربع سنوي) وإرسال النموذج المستوفى إلى Citi في غضون الأربعة عشر (14) يومًا التقويمية التالية لآخر الموعدين التاليين:

أ. إغلاق ربع السنة الذي تقدم خلاله Citi "نموذج ملف تعريف التنوع المستوى 2" إلى المورّد، أو
ب. التاريخ الذي يتلقى فيه المورّد "نموذج ملف تعريف التنوع المستوى 2" من Citi.

سوف تحتفظ Citi بجميع "نماذج ملف تعريف التنوع المستوى 2" وتعاملها وفقًا لالتزامات السرية الخاصة بـ Citi على النحو المنصوص عليه في الملحق (هـ). وسوف يرسل المورّد جميع "نماذج ملف تعريف التنوع المستوى 2" المستوفاة إلى عناية برنامج تنوع الموردين لدى شركة Citi، على 388 Greenwich Street, 19th Floor, New York, NY 10013, وعناية مدير برنامج تنوّع الموردين.

تتوفر المزيد من المعلومات على موقع مزاولة الأعمال مع شركة Citi، حيث يمكن أن تجد وصفًا لتوقعات شركة Citi الإضافية تجاه المورّدين في:

بيان Citi الخاص بمبادئ المورّدين
استراتيجية التقدم المستدام من Citi
إطار السياسة البيئية والاجتماعية
بيان حقوق الإنسان لدى Citi

6 حظر الرق الحديث

تلتزم Citi بتطبيق أنظمة وضوابط تهدف إلى تحديد ومعالجة خطر حدوث أشكال الرق المعاصرة والاتجار بالبشر في أي مكان داخل مؤسستها أو في أي من سلاسل التوريد التابعة لها. يلتزم جميع موردي Citi بالمتطلبات الموضحة أدناه، وبتطوير سياسات وإجراءات فعالة على مستوى المؤسسة لتحديد ومعالجة مخاطر الرق الحديث والاتجار بالبشر ضمن عملياتهم وسلاسل التوريد الخاصة بهم. يجب على المورّدين إكمال استبيان مسؤولية الشركات الخاص بـ Citi (ويُشار إليها باسم Corporate Responsibility Questionnaire) بناءً على طلب Citi لتمكين Citi من تقييم التعرض للمخاطر والخطوات المحتملة لتخفيف تلك المخاطر، خاصة للمورّدين في القطاعات والمناطق الجغرافية ذات المخاطر العالية.

1.6 تجنب عمالة الأطفال. لا يجوز للمورد توظيف العمالة من الأطفال. وتشير كلمة "الطفل" إلى أي شخص يقل عمره عن 15 عاماً (أو 14 عاماً حيثما يسمح قانون البلد بذلك) أو يكون تحت سن استكمال التعليم الإلزامي أو دون الحد الأدنى لسن العمل في البلد، أو أيهما أصغر. ورهناً بالحظر السائد على استخدام عمالة الأطفال، إذا تم توظيف عاملين دون سن الثامنة عشرة، يجب إيلاء عناية خاصة للواجبات التي يقومون بها والظروف التي يُطلب منهم العمل فيها لضمان عدم إصابتهم بأي ضرر بدني أو نفسي أو غير ذلك كنتيجة مباشرة أو غير مباشرة لعملهم أو الظروف التي يعملون فيها.

2.6 حرية اختيار العمل. يجب على المورّد ضمان عدم إرغام العمال أو إجبارهم نفسيًا أو جسديًا أو استعبادهم أو إجبارهم أو إلزامهم أو إخضاعهم للعمل القسري الإلزامي أو الذي يُمثل استرقاقاً لهم أو اِتجاراً بهم أو يعرضهم للعمل الإجباري بأي شكل من الأشكال، بما في ذلك العمل الإضافي القسري. ويجب أن يتم القيام بجميع الأعمال طواعيةً. تشمل التزامات المورّد بموجب هذه الاتفاقية، على سبيل المثال لا الحصر، ضمان ما يلي:

أ. **العقود والأجور وساعات العمل:** يجب توثيق شروط العمل أو التكليف للعمال في مستند خطي سهل الفهم بالنسبة لهم يحدِد بوضوح حقوقهم والتزاماتهم. ويجب أن تتضمن هذه الوثيقة الخطية، على سبيل المثال لا الحصر، شروطاً شفافة فيما يتعلق بالأجور وأجر العمل الإضافي وفترات صرف المستحقات وساعات العمل والحقوق في فترات الراحة والإجازات. تُقدم هذه الشروط المكتوبة للعامل قبل بدء عمله ويلتزم بها صاحب العمل ويجب أن تفي بمعايير الصناعة والحد الأدنى من متطلبات القوانين المعمول بها والاتفاقيات الجماعية في المكان الذي يُنفذ فيه العمل.

ب. **الحق في حرية إنهاء العمل:** يجب أن يحتفظ العمال بالحق في إنهاء عملهم بحرية، بحسب الاقتضاء، بعد فترة إخطار معقولة وفقا للقوانين المعمول بها والاتفاقيات الجماعية ودون فرض أي عقوبات غير مناسبة.

ج. **المعاملة غير الإنسانية:** لا يجوز أن يتعرض العمال وأسرهم والأشخاص المرتبطون بهم بشكل وثيق لمعاملة قاسية أو غير إنسانية، بما في ذلك، على سبيل المثال لا الحصر، العقاب البدني أو العنف أو الإكراه البدني أو النفسي أو الجنسي أو الإساءة اللفظية أو المضايقة أو التخويف. وينبغي ألّا يتعرض العمال الوافدون وأسرهم والأشخاص المرتبطون بهم بشكل وثيق للتمييز في شروط وأحكام عملهم على خلفية جنسيتهم.

د. **الأجور والمزايا وساعات العمل:** يُحدَّد أجر الموظف وفقًا لجميع قوانين الأجور المعمول بها، وتشمل تلك القوانين المتعلقة بالحد الأدنى للأجور وساعات العمل الإضافية والمزايا المقررة قانونًا. ينبغي أن يتمتع الموظفون بالقدرة على كسب أجور عادلة، وفقًا لما يحدده القانون المحلي المعمول به. وينبغي ألا تتجاوز أسابيع العمل الحد الأقصى الذي حدده القانون المحلي.

ه. **عدم مصادرة وثائق إثبات الهوية:** لا تجوز مصادرة أو احتجاز بطاقة هُوية العمال أو تصاريحهم أو جوازات سفرهم أو وثائقهم الرسمية الأخرى أو أي أشياء أخرى ذات قيمة كشرط للتوظيف، ولا يجوز أن يُستخدم احتجاز الممتلكات بصورة مباشرة أو غير مباشرة لتقييد حريات العمال أو إدخال الاستعباد إلى مكان العمل.

و. **عدم فرض رسوم توظيف أو استعباد المدين** لا يتحمل العمال، سواءٌ كان ذلك بشكل مباشر أو غير مباشر، الرسوم أو التكاليف المرتبطة بتعيينهم (بما في ذلك، على سبيل المثال لا الحصر، الرسوم المتعلقة بتأشيرات العمل وتكاليف السفر وتكاليف تجهيز الوثائق). وبالمثل، يُحظر إلزام العمال بتقديم مدفوعات يُقصد بها أو تتسبب في خلق عبودية في مكان العمل، بما في ذلك المدفوعات الأمنية أو مطالبتهم بتسديد الديون عن طريق العمل. وإذا تقرر أن العاملين قد تحملوا أي رسوم أو مصاريف فيما يتصل بعملية الاستقطاب والتوظيف، أو أي رسوم أو مصاريف أنفقت خلال عملية التوظيف، فينبغي أن يسعى المورّد إلى رد هذه التكاليف إلى العاملين. عندما تقتضي الضرورة الاستعانة بالعمال الذين يتم توظيفهم من خلال طرف ثالث، كوكالة توظيف مثلاً، فيجب ألّا يُكلف بذلك إلا وكالات التوظيف حسنة السمعة. وفي الحالات التي يتم فيها الاستعانة بالعمال مباشرةً، يجب أيضاً عدم تكليف سوى وكالات الاستقدام حسنة السمعة.

ز. **حرية الحركة:** للعمال الحق في الحركة دون قيود غير معقولة ويجب ألا يتم حصرهم جسديًا في مكان العمل أو في أماكن أخرى يسيطر عليها صاحب العمل (مثل وحدات الإقامة). ويجب ألا تُوضع أي شروط تُلزم العمال بالإقامة في المنشآت التي يسيطر عليها صاحب العمل إلا إذا كان ذلك ضرورياً بسبب موقع أو طبيعة العمل المنفذ.

ح. **التظلمات دون انتقام:** للعمال الحرية في رفع الشكاوى إلى أصحاب العمل لديهم فيما يتعلق بمعاملة صاحب العمل لهم، ولا يجوز أن يتعرضوا للضرر أو الانتقام أو الإيذاء بسبب تقديم الشكاوى والتظلم.

7 موظفو المورّد

1.7 تدريب موظفي المورّد وتكليفهم وإعادة تكليفهم وإدارتهم يلتزم المورّد باستخدام أعدادًا كافية من الأفراد من ذوي المستويات المناسبة من التدريب والتعليم والخبرة والمهارة لأداء الخدمات بأكثر الطرق فعالية بما يتفق مع أي عقد، وسوف يلتزم بتقديم الأدلة الثبوتية على مؤهلات هؤلاء الأفراد عند الطلب. بعد تكليف الموظفين في المشروع، يجب على المورّد عدم إعادة تكليف أو استخدام أي موظفين في أمور أخرى تقلل من توفر أولئك الموظفين للعمل في المشروع دون موافقة كتابية مسبقة من Citi، وسوف يقوم على وجه العموم بتكليف موظفين للعمل في المشاريع بطريقة تقلل من أي اضطراريات تنتج عن الحاجة إلى إعادة التوجيه. يضمن المورّد أن موظفيه لا يعتبرون أنفسهم موظفين أو وكلاء لدى Citi، كما يضمن عدم سعي موظفيه إلى معاملتهم كموظفين في Citi لأي غرض، بما في ذلك المطالبات باستحقاق المزايا الإضافية أو المتنوعة التي تقدمها Citi، أو الدخل في حالات العجز، أو ضرائب أو مزايا الضمان الاجتماعي أو ضرائب البطالة الفيدرالية أو المزايا الحكومية للتأمين ضد البطالة أو استقطاع ضريبة الدخل الفيدرالية. يتحمل المورّد وحده المسؤولية عن جميع المسؤوليات المتعلقة بصاحب العمل فيما يتعلق بموظفيه بما في ذلك، على سبيل المثال لا الحصر، توفير جميع التغطيات التأمينية المطلوبة، وتقديم جميع الإقرارات الضريبية المعمول بها، وتنفيذ جميع المدفوعات والإيداعات الضريبية المطلوبة بطريقة تتفق مع وضعية المورّد باعتباره مقاول مستقل.

2.7 استبدال موظفي المورّد. يقوم المورّد باستبعاد واستبدال أي موظف يعينه المورّد لمشروع ما إذا أخطرت Citi المورّد بأن ذلك الموظف غير مقبول من جانب Citi لأي سبب آخر غير تمييزي. يوافق المورّد كذلك على إلغاء عمل أي موظف تم تعيينه في مشروع واستبداله وعلى منع ذلك الموظف من تقديم الخدمات إلى Citi (أو من أي مسؤولية فيما يتعلق بتقديم الخدمات أو الإشراف عليها) فورًا عندما يكون ذلك الموظف غير قادر أو غير راغب في تقديم الخدمات في الوقت المناسب وبطريقة مهنية.

3.7 سياسات شؤون الموظفين الخاصة بالمورّد. يقر المورّد ويضمن ويتعهد بأنه يضع ويدير بشكل فعال سياسات وإجراءات شاملة لتأهيل موظفيه الذين هم أشخاص طبيعيون ومكلفون بتقديم خدمات في الموقع إلى Citi، وأن هذه السياسات والإجراءات تشمل التحقق من ترخيص العمل، وفحص التاريخ الوظيفي السابق والإدانات الجنائية للموظف، على النحو المنصوص عليه في هذه الوثيقة، واختبار المخدرات قبل إلحاق الموظف بالعمل، كل ذلك إلى الحد الذي يسمح به القانون المعمول به وأي اتفاقية عمل جماعية سارية. دون تقييد عمومية ما سبق، يُقر المورّد كذلك ويضمن ويتعهد بأن لديه ضوابط وإجراءات لضمان امتثال المورّد الكامل لجميع القوانين المعمول بها المتعلقة بالهجرة، بما في ذلك التحقق من أن جميع موظفي المورّدين المكلفين بأعمال Citi مصرح لهم بالعمل طوال المهمة على نحو يتسم بالامتثال الكامل لجميع القوانين المعمول بها المتعلقة بالهجرة. بناءً على طلب Citi، يقدم المورّد إلى Citi على الفور دليلًا كتابيًا على تصريح العمل لأيٍ من أو جميع موظفي المورّدين المكلفين بأعمال Citi وامتثالهم للقانون المعمول به فيما يتصل بالهجرة، ويقوم المورّد بتغيير أي موظف ليس لديه تصريح عمل متوافق مع القانون المعمول به ببديل مناسب يحل محل ذلك الموظف، بما في ذلك توفير كل ما يلزم من تدريب وتوجيه لضمان توفير الخدمات في الوقت المناسب وبشكل فعال، وذلك في كل حالة دون أي تكلفة إضافية على Citi.

8 مكافحة الاحتيال

1.8 فيما يتعلق بجهود Citi لتحديد مخاطر الاحتيال والتخفيف من حدتها (يُشار إليها باسم "مكافحة الاحتيال"). **يجب على جميع المورّدين:**

أ. التعاون مع أي تحقيقات تجريها Citi بشأن أي سرقة مشتبه بها أو مزعومة أو احتيال أو أي نشاط إجرامي أو أي مخالفة محتملة أخرى، وأي محاكمة بشأن أي سلوك احتيالي أو إجرامي إلى أقصى حد يسمح به القانون؛

ب. وضمان إبلاغ Citi في الوقت المناسب عن أي حوادث احتيال محتملة. ويشمل هذا، على سبيل المثال لا الحصر، محاولة السرقة أو الاحتيال (مثل إرسال بيانات خاطئة أو غير دقيقة أو مُحرفة بشأن المورّد، أو أنظمة الفوترة، أو اختفاء الأموال أو الأوراق المالية، إلخ) أو النشاط الإجرامي أو المخالفة الإجرامية أو الاشتباه في حدوث أيٍ مما سبق أو ادعائه أو وقوعه فعلاً مما يتضمنCiti أو أحد موظفيها أو مورّديها أو وكلائها أو التابعين لها من غير موظفيها (كالموظفين المؤقتين أو المتعاقدين)؛

ج. والسماح بإجراء المراقبة والإشراف من قبل شركة Citi وممثليها ودعم شركة Citi - وإنفاذ القانون - مما يؤدي إلى إجراء تحقيقات في نشاط الاحتيال المحتمل والذي يتورط فيه هذا المورّد؛

د. والإبلاغ، في الوقت المناسب، عن أي تضارب في المصالح (بما في ذلك تضارب المصالح بين المورّدين/موظفي المورّد و/أو موظفي Citi) التي يتم إعلام المورّدين بها؛

ه. ودعم إجراءات مكافحة الاحتيال في Citi أثناء إعداد أو تحديث الحساب المصرفي للمورد في نظام الدفع الخاص بموردي Citi.

2.8 وإضافةً إلى ذلك، **يتعين** على المورّدين الذين يقدمون خدمات تكون بطبيعتها أكثر عرضة لمخاطر الاحتيال القيام بما يلي:

أ. توثيق واتباع برنامج إدارة مخاطر الاحتيال الذي يحدد مخاطر الاحتيال الجوهرية ذات الصلة بالخدمات التي يقدمونها لشركة Citi وكذلك الضوابط والإجراءات المعمول بها للتخفيف من هذه المخاطر؛

ب. وتدريب كامل على التوعية بالاحتيال (في غضون 90 يومًا تقويميًا من التعيين وسنويًا بعد ذلك) وتدريب الموظفين على عناصر مخاطر الاحتيال المحددة ذات الصلة بالخدمات المحددة التي تقدمها شركة Citi؛

ج. ورصد حالات محاولات الاحتيال والالتزام بالضوابط الفعالة للتخفيف من مخاطر الاحتيال على الخدمات التي يقدمونها لشركة Citi، وتوثيق إجراءات الضوابط واختبار مدى فعالية الضوابط على أساس مستمر، مع الإبلاغ عن أي أوجه قصور إلى مسؤول النشاط التجاري (BAO).

3.8 يشمل المورّدون المعرضون لمخاطر احتيال أعلى بطبيعة عملهم، على سبيل المثال لا الحصر:

أ. من يمكنهم الوصول إلى البيانات المصنفة باعتبارها سرية أو عليا (عندما لا تخضع للرقابة أو الإشراف المباشرين من Citi) والتي يمكن استخدامها لتمكين الاحتيال مثل الوصول إلى الحسابات الداخلية، والمعاملات المالية، المعاملات النقدية؛

ب. ومن لديهم اتصال بشبكات/أنظمة Citi؛

ج. ومن يقدمون أو يدعمون أو يمكنهم الوصول إلى الخدمات والإمكانات التي تكون مصدر استهداف لارتكاب الاحتيال أو تمكينه، بما في ذلك:

1. طلبات تحديد الهوية، أو الالتحاق بعمل، أو معالجة من عملاء جدد؛
2. أنشطة تحويل مدفوعات/أموال من Citi أو العملاء، و/أو مصادقة وصول عملاء Citi لهذه الخدمات؛
3. إجراء تغييرات على بيانات Citi أو البيانات القائمة بين شركة Citi والعملاء (مثل البيانات الديموغرافية) أو التحقق منها أو تنفيذها؛
4. توفير أدوات معاملات أو تقديم خدمات بشأنها أو مصادقتها (مثل بطاقات الخصم/ الائتمان، المحافظ الإلكترونية، دفاتر الشيكات، وغيرها)؛
5. توفير أنشطة إدارة الاحتيال التشغيلية إلى Citi أو دعمها، والتي تختص بمنع حوادث الاحتيال أو اكتشافها أو الاستجابة لها؛
6. توفير الوصول المادي إلى النقد والصكوك المالية والأصول/ السلع المادية؛
7. الدخول دون مُرافق أو خارج ساعات العمل إلى مرافق Citi؛
8. البيانات المالية: أنشطة المحاسبة، مثل إضافة مدخلات إلى دفتر الأستاذ العام أو الفرعي؛
9. كسب أو إنفاق مكافآت للأنشطة المُحفّزة.

9 التفاعل مع وسائل الإعلام والظهور العام

إن إدارة الشؤون العامة العالمية لدى Citi هي الإدارة الوحيدة المُخوّلة بإصدار البيانات الصحفية أو التصريحات العامة نيابةً عن Citi. ولا يجوز للمورّدين إصدار أي بيان صحفي يُشير بشكل مباشر أو غير مباشر إلى Citi أو أي عقد أو اتفاقية بين أحد المورّدين وCiti أو أي منتجات وخدمات تشتريها Citi من المورّد. ولا يجوز للمورّدين الموافقة على أو المشاركة في أي نشاط من أنشطة العلاقات العامة يتعلق بشركة Citi مع العملاء أو موظفيها أو مورّديها الآخرين أو العملاء الآخرين للمورّدين أو أي أطراف ثالثة دون الحصول على موافقة كتابية مسبقة من جهة الاتصال الرئيسية للأعمال في Citi.

لا يجوز للمورّدين إعلان أو نشر أي مادة بصيغة خطية أو إلكترونية (بما في ذلك الكتب والمقالات وعمليات التدوين الصوتي وعمليات البث الشبكي والمدونات والموضوعات المُحملة على مواقع الويب والصور ومقاطع الفيديو ووسائل الإعلام الاجتماعي وغيرها) أو ذكر اسم Citi أو عملياتها أو عملائها أو منتجاتها أو خدماتها في أي لقاءات أو مقابلات أو في فعالية عامة دون الحصول على موافقة كتابية مُسبقة من جهة الاتصال الرئيسية للأعمال في Citi والمسؤول الأول للشئون العامة القُطرية أو الإقليمية.

ولا يجوز للمورّدين، سواءٌ فيما يتعلق بتقديم الخدمات أو المنتجات لشركة Citi أو غير ذلك، استخدام الإشارات المُميزة أو العلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو الشعارات أو الرموز أو أسماء العلامات الخاصة بشركة Citi دون الحصول في كل حالة على موافقة كتابية مسبقة منها. لا يجوز للمورّدين استخدام اسم Citi أو شعارها أو علاماتها التجارية أو منشآتها أو علاقاتها لتحقيق فائدة أو للعمل خارج Citi (بما في ذلك في رأسية الخطابات أو مواقع الويب الشخصية أو المدونات أو مواقع شبكات التواصل الاجتماعي الأخرى). وعلاوة على ذلك، لا يجوز للمورّدين استخدام اسم Citi أو منشآتها أو علاقاتها للأغراض الخيرية أو التطوعية.

10 الاتصالات الإلكترونية المكتوبة

عند التعامل مع موظفي Citi أو عند تأدية التزاماتهم لصالح شركة Citi أو نيابةً عنها، لا يُسمح للمورّدين إلا باستخدام معدات وأنظمة وخدمات الاتصالات الإلكترونية التي توفرها شركة Citi وتصادق عليها وتعتمدها. يجب الموافقة على قنوات الاتصالات الإلكترونية الجديدة أو الموسعة أو المعدلة الخاصة بـ Citi، سواء كأداة مستقلة أو مدمجة في منصة أوسع توفرها Citi أو يوفرها طرف ثالث وفقًا لمتطلبات Citi المعمول بها الواردة في هذه الوثيقة، أو التي تم إخطار المورّد بها كتابةً من قبل مسؤول النشاط التجاري الخاص به. يحظر إجراء مراسلات بين شركة Citi وموظفيها عبر منصات مراسلات غير التي تعتمدها Citi مثل WhatsApp وWeChat وأي منصة إلكترونية تفاعلية أخرى.

وإضافةً لذلك، ينبغي ألا يكون لدى الموردين أي توقع بشأن الخصوصية فيما يتعلق بالاتصالات الإلكترونية المكتوبة التي أنشأتها أو اكتشفتها أو استخدمتها أو وصلت إليها أو نزّلتها أو خزّنتها أو نقلتها أو استقبلتها أو حذفتها معدات وأنظمة وخدمات الاتصالات التي توفرها Citi. ويجوز لشركة Citi مراقبة مُعدات وأنظمة وخدمات الاتصالات الإلكترونية، فضلاً عن الاتصالات الإلكترونية نفسها. فهذه الاتصالات الإلكترونية تخضع لملكية Citi ويجوز الاحتفاظ بها وفقًا لمتطلبات الاحتفاظ بالسجلات المعمول بها (وفقًا للقانون واللوائح المحلية).

11 الأنشطة والمساهمات السياسية

توجد مجموعة متنوعة من القوانين، مثل تمويل الحملات والهدايا والأنشطة الترفيهية وممارسة الضغط التشريعي والتنظيمي والمشتريات والدفع مقابل اللعب والأوراق المالية، التي تنظم الأنشطة السياسية التي تزاولها شركة Citi ومورّدوها. ويحظر على المورّدين مزاولة أي نشاط سياسي لا يمتثل لسياسة أو معايير Citi ذات الصلة أو القانون أو اللوائح المعمول بها.

يشمل النشاط السياسي على سبيل المثال لا الحصر:

أ. تقديم مساهمات سياسية مؤسسية أو شخصية أو التماس مساهمات سياسية أو استخدام أموال الشركة أو مواردها (مثل المرافق أو المعدات أو البرامج أو الموظفين) أو التطوع في الخدمات الشخصية خلال وقت العمل بالشركة نيابةً عن أي مرشح يدشن حملة انتخابية لتولي منصب عام أو لجنة حزب سياسي أو لجنة سياسية؛

ب. أو المشاركة في أنشطة كسب تأييد أو دعاية لمسؤولين حكوميين، سواءٌ كان بشكل مباشر أو من خلال أطراف ثالثة، بما في ذلك محاولات التأثير على التشريعات والتي قد تشمل، حسب الاختصاص القضائي، محاولات التأثير على وضع قواعد الوكالة أو ترسية عقود حكومية؛

ج. أو السعي إلى تولي منصب سياسي مرتبط بالحكومة أو قبوله أو شَغله، بما في ذلك أي مجلس أو لجنة حكومية أو أي مؤسسة مماثلة أخرى.

ولا يجوز لأي مورّد الاضطلاع بأي نشاط سياسي أو القيام به نيابةً عن (أو بزعم أنه نيابةً عن) Citi دون الحصول على تصريح كتابي مسبق من مكتب مراقبة العمليات العالمية للشؤون الحكومية العالمية لدى Citi من خلال (ggacontrol@citi.com). ورغم أن Citi قد تدفع رسوم و/أو تسدد تكاليف عينية لخدمات الأنشطة السياسية المتعاقد عليها والمسموح بها التي يقدمها المورّد مثل ممارسات الضغط، فإن شركة Citi لن تعوض مطلقًا أي مورّد أو أي من موظفيها عن أي من المساهمات السياسية الشخصية أو المؤسسية أيًا كان نوعها.

12 مكافحة غسل الأموال ("AML")

ينطبق على المورّدين الذين يؤدون خدمات معينة تتعلق بالعملاء (مثل الالتحاق بالخدمة وحساب العميل وفحص المعاملة) أو تسليم البيانات/المقاييس المتعلقة بالأنشطة السابقة؛ و/أو الذين يعملون كوسيط فيما يتعلق بالنقد أو الأدوات المالية (مثل خدمات استقبال الإيداع عن بعد أو البريد السريع أو سيارات نقل الأموال المصفحة أو الخزائن المصفحة).

1.12 الالتزامات المتعلقة بمكافحة غسل الأموال:

أ. الحفاظ على عمليات وإجراءات Citi والامتثال لها والتي تكون مُخصصة لتلبية متطلبات القوانين المعمول بها والامتثال لها، وتشمل (1) قانون جرام-ليش-بليليي واللوائح الصادرة بموجبه؛ (2) وقانون باتريوت الولايات المتحدة الأمريكية واللوائح الصادرة بموجبه؛ (3) وأي قانون أو لوائح تختص بغسيل الأموال؛ (4) وأي قانون أو لوائح ذات صلة بالعقوبات الاقتصادية. تناول هذه السياسات والإجراءات للأدوار والمسؤوليات التي تتبنى مكافحة غسل الأموال، بما في ذلك متطلبات الإبلاغ الفوري عن أي نشاط ترصده ويوحي بممارسات غير اعتيادية أو يُحتمل كونها غير اعتيادية ذات صلة بتدفق النقد؛

ب. ضمان حصول موظفيها الذين يقدمون الخدمات إلى Citi على تدريب سنوي فيما يخص الأدوار والمسؤوليات التي تتبنى مكافحة غسل الأموال، بما في ذلك متطلبات الإبلاغ الفوري عن أي نشاط ترصده ويوحي بممارسات غير اعتيادية أو يُحتمل كونها غير اعتيادية فيما يتصل بتدفق النقد. يمكن أن يشتمل التدريب على عناصر مثل:

1. الإبلاغ عن النشاط المشتبه به وتصعيده
2. برنامج "اعرف عميلك"، ويشمل برنامج تحديد هوية العميل، وفحص العقوبات والأسماء، والعناية الواجبة للعميل، والعناية الواجبة المعززة
3. مراقبة المعاملات
4. الإبلاغات/القياسات الدورية، بما في ذلك الإبلاغ عن التغييرات القانونية والتنظيمية والتغييرات الجوهرية في برنامج مكافحة غسل الأموال
5. اختبار مدى فعالية برنامج مكافحة غسل الأموال ووضع ضوابط له، بما في ذلك زيارات الموقع

ج. الامتثال لأي أحكام تعاقدية تحدد أي برنامج لمكافحة غسل الأموال يجب أن يضعها المورّد.

د. إبلاغ شركة Citi كتابيًا على الفور عن أي انتهاكات مشتبه بها للقانون، بما في ذلك أي نشاط ترصده ويوحي بممارسات غير اعتيادية أو يُحتمل كونها غير اعتيادية ذات صلة بتدفق النقد فيما يتعلق بـ Citi أو عملائها.

ه. الامتثال لقوانين ولوائح الضرائب المعمول بها في البلدان التي يعملون فيها. ولا ينبغي بأي حالٍ من الأحوال أن يتورط المورّدون في التهرب الضريبي المتعمد غير المشروع أو تسهيل هذا التهرب نيابةً عن الآخرين والذي قد يشمل التورط في أنشطة من شأنها المساعدة في التهرب من مدفوعات الضرائب المستحقة وواجبة الدفع أو إخفاء معلومات عن السلطات الضريبية. وكذلك، يجب أن يتبني المورّدون إجراءات وقائية معقولة ذات صلة بالتهرب الضريبي وأن يبلغوا شركة Citi كتابةً وفوراً بأي انتهاكات فعلية أو مشتبه فيها تتعلق بشركة Citi.

2.12 يجب على المورّدين وضع سياسات وإجراءات داخلية مناسبة للامتثال لجميع قوانين ولوائح مكافحة غسل الأموال الموجودة الآن أو التي سيتم تفعيلها فيما بعد.

13 إدارة السجلات

تسري على المورّدين الذين يقومون بالوصول إلى معلومات Citi ومعالجتها وتخزينها.

تطلب Citi من جميع المورّدين الذين بعهدتهم معلومات خاصة بشركة Citi العمل مع مسؤول النشاط التجاري (BAO) الخاص بهم أو جهة الاتصال الرئيسية للأعمال في Citi من أجل (أولاً) تحديد وتصنيف المعلومات كسجلات أو على أنها مؤقتة لأغراض إدارة السجلات الخاصة بشركة Citi؛ (ثانيًا) وتصنيف السجلات وفقًا لكتالوج السجلات الرئيسي (MRC) الخاص بشركة Citi؛ (ثالثًا) والاحتفاظ بالمعلومات استنادًا إلى متطلبات الاحتفاظ؛ (رابعًا) وفي حالة عدم وجود أمر احتفاظ بالسجلات، التخلص من المعلومات بشكل مناسب في نهاية دورة حياتها.

يجب أن يعمل المورّدون مع جهة الاتصال الرئيسية للأعمال في Citi أو مسؤول النشاط التجاري لضمان أن قائمة السجلات تحدد وتصنف السجلات وفقًا لرموز السجلات الخاصة بشركة Citi في كتالوج السجلات الرئيسي وأنه يتم تحديثها بشكل سنوي على الأقل. ويلتزم المورّد بالتقيد بمتطلبات إدارة السجلات التي يتم إبلاغه بها من جانب مسؤول النشاط التجاري. يجب التخلص من السجلات والمعلومات التي تفي بالتزام الاحتفاظ المُدرجة في كتالوج السجلات الرئيسي (MRC) ولا تخضع لأحكام الاحتفاظ بالسجلات، في غضون عام واحد منذ أن تصبح مؤهلة للتخلص منها. يجب التخلص من السجلات الخاضعة للائحة العامة لحماية البيانات (GDPR) في غضون 6 أشهر منذ أن تصبح مؤهلة للتخلص منها، ما لم تكن خاضعة لأحكام الاحتفاظ بالسجلات. ويجب على المورّد تعليق إتلاف أو تغيير معلومات Citi بمجرد إخطاره بحفظ السجل. ويجب إتلاف المعلومات المؤقتة بعد مدة لا تزيد عن عامين من آخر استخدام لها ما لم تخضع لأحكام الحجز. كما يجب على المورّد التحقق من جهة الاتصال الرئيسية للأعمال في Citi الخاصة به أو مسؤول النشاط التجاري (BAO) في حالة وجود أي شك لديه.

يتحمل المورّدون الذين يحتفظون بالوثائق نيابةً عن Citi مسؤولية الحفاظ على جميع المعلومات (يُشار إليها باسم "الاحتفاظ") وجمعها وإنتاجها، والتي تعتبر ذات صلة بإجراء قانوني أو أي إجراء آخر خلال الوقت المطلوب وفقًا لما يطلبه مسؤول النشاط التجاري (BAO).

يجب على المورّدين عدم التخلص من أي من معلومات Citi، بغض النظر عن تصنيفها (سواءٌ كانت سرية أو غير سرية) دون الحصول على موافقة جهة الاتصال الرئيسية للأعمال في Citi أو مسؤول النشاط التجاري (BAO)، ويجب أن تتضمن تلك الموافقة التأكيد على عدم وجود أي أمر احتفاظ بشأن المعلومات التي سيتم التخلص منها. وتظل متطلبات إدارة السجلات والاحتفاظ بها وجميع متطلبات مناولة المعلومات الأخرى سارية بعد إنهاء العقد أو انتهائه ما لم يتم الاتفاق صراحةً على غير ذلك.

يحتفظ المورّدون بوثائق تضم جميع موظفيهم المسؤولين عن الإشراف على إدارة معلومات Citi الموجودة في عهدة المورّد وعليهم عقد اجتماعات دورية مع جهة الاتصال الرئيسية للأعمال في Citi أو مسؤول إدارة السجلات لمراجعة أسماء جهات الاتصال والتفاصيل الإجرائية والأدوار والمسؤوليات وقائمة سجلات المورّد وتحديثها.

14 خدمات التعامل مع العملاء

تسري على تعاملات المورّد مع أي فرد بصفته عميلاً سابقًا أو حاليًا أو محتملًا لـ Citi أو لطرف ذي صلة (مثل موظف أو ممثل) لهذا العميل (يُشار إلى كل فرد من هؤلاء باسم "العميل").

1.14 ساعات العمل. يجب على المورّد توجيه واستخدام الجهود المعقولة لضمان ألا يحاول موظفوه الذين يعملون في منشآت Citi الوصول إلى منشآت Citi خارج ساعات العمل العادية (أو في عطلة محددة) لتلك منشآت، وكذلك التعاون مع التعليمات المتعلقة بالأمن الخاصة بموظفي Citi والامتثال لتلك التعليمات.

2.14 السياسات والإجراءات. فيما يتعلق بخدمات التعامل مع العملاء فقط: يقر المورّد ويوافق على أن التزامه بموجب أي عقد بأن يجعل موظفيه العاملين في منشآت Citi يلتزمون بالامتثال لسياسات وإجراءات مكان العمل الخاصة بـ Citi يتضمن الامتثال لإجراءات الأمان المادي وغيرها من التدابير الأمنية الخاصة بـ Citi والشركات التابعة لها. تبذل Citi جهودًا معقولة لإبقاء المورّد على اطلاع بجميع إجراءات الأمان المادي والتدابير الأمنية الأخرى. تتمتع Citi بالسلطة التقديرية لإصدار وتفعيل ومصادرة وإلغاء تنشيط بطاقات التعريف أو المفاتيح أو غيرها من الأجهزة الأمنية إلى موظفي المورّد العاملين في منشآت Citi أو من هؤلاء الموظفين؛ شريطة ألا يُنظر إلى قيام Citi بهذه الإجراءات على أنه ينطوي على أي علاقة عمل بين Citi وهؤلاء الأفراد.

3.14 خطة التعافي من الكوارث. يضع المورّد خطة طوارئ (يُشار إليها باسم "خطة التعافي من الكوارث") لمواصلة العمل (ويقدم دليلًا على اختباراته الحالية والدورية لتلك الخطة إذا طلبت Citi ذلك) وبهذا يكون المورّد، وعلى الرغم من أي اضطراب في قدرة المورّد على توفير الخدمات أو أداء الالتزامات الأخرى بموجب هذه الاتفاقية من أي موقع معين أو من خلال جهود أي أفراد معينين، قادرًا على أن يقوم على الفور بتوفير الخدمات وتنفيذ التزاماته من موقع بديل أو باستخدام موظفين بدلاء. يجب تقديم نسخة من خطة التعافي من الكوارث إلى Citi في غضون عشرة (10) أيام تقويمية من تاريخ سريان كل أمر عمل يتم الدخول فيه بين Citi والمورّد لتوفير "خدمات التعامل مع العملاء"، وسنوياً بعد ذلك طالما يسري مفعول كل أمر عمل. يزوّد المورّد Citi بأي تعليمات أو معلومات أخرى ضرورية لأن تستمر Citi في تلقي الخدمات من المورّد في ظل الظروف التي يتعين على المورّد فيها استدعاء خطة التعافي من الكوارث الخاصة به. يقر المورّد ويضمن ويتعهد بأن خطته للتعافي من الكوارث سوف تشمل، على الأقل، ما يلي:

أ. صيانة المورّد لموقع ثانوي للتعافي من الكوارث منفصل عن مواقع الخدمة، وتخزين وسائط النسخ الاحتياطي في موقع منفصل عن مواقع الخدمة، واستخدام خطوط وخوادم اتصالات إضافية وخلافه؛

ب. وإجراءات النسخ الاحتياطي/استعادة تشغيل الخدمات وتطبيقها، بما في ذلك خطة مفصلة وموثقة للاستجابة للانقطاع المطول في الخدمات الناتج عن انقطاع التيار الكهربائي أو تعطل النظام أو الكوارث الطبيعية أو غيرها من الظروف غير المتوقعة التي تتضمن عمليات وإجراءات خاصة باستئناف العمليات في غضون فترة زمنية يتفق عليها الطرفان؛

ج. وإجراءات حماية جميع المحتوى؛

د. والإجراءات وأي اتفاقيات مع طرف ثالث لاستبدال المعدات (مثل أجهزة الكمبيوتر)،

ه. والإجراءات الخاصة بأي منشآت إنتاج خارج الموقع. وإضافةً لذلك، ستنص خطة التعافي من الكوارث الخاصة بالمورّد على ما يلي:

1. أن يخطر المورّد Citi كتابيًا في غضون ساعتين (2) من أي كارثة يمكن أن تؤثر سلبًا على الخدمات؛
2. وأن يقدم المورّد لشركة Citi، في غضون 24 ساعة من الإشعار المذكور، خطة لمواصلة تقديم الخدمات في منشأة معالجة بديلة،
3. ووجوب معاودة الخدمات للعمل بشكل كامل في غضون 48 ساعة من الإشعار الأولي. يوافق المورّد، عند الطلب، على إصدار المعلومات اللازمة التي تتيح لـ Citi تطوير خطة التعافي من الكوارث وخطة استمرارية الأعمال والتي ستعمل بالتنسيق مع خطة التعافي من الكوارث الخاصة بالمورّد وخطة استمرارية الأعمال. يوافق المورّد على اختبار خطته للتعافي من الكوارث سنويًا، وعند الطلب، يقدم تقريرًا مكتوبًا عن نتائج اختبار التعافي من الكوارث إلى Citi. وفي حالة تعطل أجزاء من منشآت المورّد، سيعامل المورّد Citi على نحو لا يقل تفضيلًا عن معاملة المورّد لعملائه التجاريين الآخرين. يلتزم المورّد بأن يضمن أن أي مقاول من الباطن تابع للمورد يحتفظ بخطة للتعافي من الكوارث وغيرها من الإجراءات والضوابط التي تتوافق تمامًا مع أحكام ومتطلبات هذا القسم.

4.14 شهادة العناية الواجبة. يقر المورّد بأن Citi والشركات التابعة لها مطالبون بإجراء العناية الواجبة المنتظمة لمورديها الذين يقدمون "خدمات التعامل مع العملاء" من خلال استبيان/شهادة سنوية (يُشار إليها باسم "شهادة العناية الواجبة") التي تتناول:

أ. تراخيص الأعمال الخاصة بالمورّد (بما في ذلك عقود التأسيس، وشهادات حسن السمعة، وأي تراخيص مطلوبة سارية)،

ب. وامتثال المورّد للقانون المعمول به،

ج. والتغطية التأمينية،

د. والمهارات والمؤهلات والخبرة

ه. وقدرة المورّد (بما في ذلك مستويات التوظيف وموازنة عبء العمل)،

و. وإجراءات الأعمال ذات الصلة،

ز. وممارسات التعويضات،

ح. والجدوى المالية ومخاطر الطرف المقابل،

ط. ومخاطر السمعة (الشكاوى/الدعاوى القضائية الوشيكة)،

ي. والسياسات والممارسات التي تنظم التعامل مع العملاء،

ك. ومراجع المورّد،

ل. وعلاقة المديرين،

م. والاعتماد على المقاولين من الباطن أو المقاولين أو أي موفري الخدمات الخارجيين،

ن. ومراجعة برنامج التدريب،

س. وخطة استمرارية الأعمال،

ع. ونتائج تدقيق الجودة والامتثال لأي التزامات مستوى الخدمة المعمول بها،

ف. وإدارة المستندات وتخزينها.

يقوم المورّد، من وقت لآخر، بتزويد Citi بأي معلومات أو مستندات أخرى قد تطلبها Citi لضمان الامتثال (1) لأي عقد، (2) ولسياسات الشركات المتبعة لدى Citi، (3) وللمتطلبات التنظيمية المطبقة على Citi والمورّد.

5.14 الأمان. في حالة الاحتفاظ بأي معلومات سرية أو تخزينها بأي طريقة على موقع ويب أو نظام يمكن الوصول إليه عبر الويب، يجب على المورّد الإفصاح إلى Citi عن ذلك، ويجوز إدراج ذلك الإفصاح في وصف الخدمات. في حالة احتفاظ المورّد بمعلومات Citi السرية أو تخزينها على النحو المتوخى أعلاه، فإن المورّد؛

أ. يلتزم بإجراء تدقيق (البيان رقم 16 حول معايير التزامات المصادقة) SSAE 16 (أو أي إرشادات موثوقة لاحقة لتقديم التقارير حول مؤسسات الخدمة) مرة واحدة سنويًا خلال مدة هذه الاتفاقية، (ب) وكما يلتزم بأن يقدم إلى Citi، مرة واحدة سنويًا على الأكثر، نسخة من التقارير التي يتلقاها المورّد فيما يتعلق بالامتثال لـ SSAE 16 (أو أي إرشادات موثوقة لاحقة للإبلاغ عن مؤسسات الخدمة)؛

ب. يمتثل لمعايير إدارة أمان المعلومات ISO / IEC 207002 (معيار لأمان المعلومات تنشره المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الدولية للتقنيّات الكهربائية (IEC)) (أو معايير إدارة أمان المعلومات اللاحقة التي تضع معايير وبروتوكولات أعلى)؛ (3) ويلتزم بأحكام أمان الكمبيوتر.

6.14 شكاوى العملاء. يخطر المورّد جهة الاتصال الرئيسية للأعمال في Citi (أو من ينوب عنه) كتابيًا في غضون أربع وعشرين (24) ساعة بأي شكاوى كتابية أو شفهية تنطوي على عدم الرضا أو القلق (يُشار إلى كل منها باسم "شكوى") يتلقاها المورّد من أي عميل أو من أي جهة تنظيمية ذات صلة فيما يتعلق بالخدمات التي يقدمها المورّد نيابةً عن Citi أو فيما يتعلق بها، بما في ذلك أي شكوى تتعلق بحيازة أو استخدام بيانات العميل أو حقوق الخصوصية للعميل. ما لم توفر Citi ذلك النظام للمورّد، فسوف يقوم المورّد أيضًا بتطوير وتنفيذ وصيانة نظام (يُشار إليه باسم "نظام التتبع") بما يحقق رضا Citi بشكل معقول لتتبع الشكاوى وتزويد Citi، وفقًا لتقديرها، بنسخة من التقارير أو بإمكانية الوصول إلى الأنظمة. يقوم نظام التتبع بالوظائف الآتية:

أ. تصنيف الشكاوى حسب النوع وتاريخ الاستلام وتاريخ تقديم إشعار الشكوى إلى Citi،

ب. وتتبع مسار التعامل مع الشكوى حتى الانتهاء/حلها،

ج. وتوفير جميع الأمور الأخرى التي قد تطلبها Citi بشكل معقول. يجب تصميم نظام التتبع بما يسمح للمورد بتحديد ما إذا كان يتلقى عددًا هائلاً من الشكاوى فيما يتعلق بمسألة معينة حتى يتمكن المورّد (بالتشاور مع Citi) من تحديد ما إذا كانت هناك مشكلة منهجية تتعلق بأعمال المورّد أو تقديمه للخدمات وليتمكن على الفور من تصحيح المشاكل.

7.14 أمان الشبكات والاتصالات. نشر طبقات دفاع متعددة بما في ذلك نشر تلك الطبقات على أنظمة المورّدين، وتشمل على سبيل المثال لا الحصر، أنظمة جدران الحماية Firewalls، وأنظمة اكتشاف اختراق الشبكة وأنظمة اكتشاف التسلل القائمة على المضيف. ويجب مراقبة جميع أنظمة المراقبة الأمنية بما في ذلك، وتشمل على سبيل المثال لا الحصر، جدران الحماية وأنظمة كشف التسلل، على مدار 24 ساعة في اليوم، 365 يومًا تقويميًا في السنة. تكوين جدران الحماية وأجهزة توجيه الشبكة والمحولات وأجهزة موازنة التحميل وخوادم الأسماء وخوادم البريد ومكونات الشبكة الأخرى وفقًا لمعايير الصناعة المعقولة من النواحي التجارية. وبناءً على طلب Citi، ووفقًا للمعلومات التي تصل إلى Citi حول نقاط الضعف والتهديدات، يتم تقييد الوصول إلى أي مكون خاص بـ Citi من الشبكات والأنظمة والتطبيقات المستخدمة لتقديم الخدمات بموجب أي عقد.

8.14 أمان منصات البنية التحتية والخدمات والعمليات. تكوين جميع أنظمة وخدمات البنية التحتية (أنظمة التشغيل وخوادم الويب وخوادم قواعد البيانات وجدران الحماية وأجهزة التوجيه وما إلى ذلك) التي تُستخدم لتقديم الخدمات بموجب أي عقد وآليات مصادقة وفقًا لأفضل الممارسات في المجال. التأكد من أن جميع حالات الوصول الإداري عن بُعد لأنظمة الإنتاج يتم إجراؤها عبر اتصالات مشفرة (مثل حلول بروتوكول النقل الآمن SSH و SCP وواجهات إدارة الويب التي تدعم SSL والشبكات الافتراضية الخاصة VPN).

9.14 أمان التطبيقات. عدم السماح إلا للمستخدمين المعتمدين والمصرح لهم بعرض أو إنشاء أو تعديل أو حذف المعلومات التي تديرها التطبيقات المستخدمة فيما يتعلق بتقديم الخدمات بموجب أي عقد. التأكد من أن ملفات تعريف الارتباط في متصفح الويب التي تخزن البيانات السرية يتم تشفيرها باستخدام خوارزمية تشفير عامة ومقبولة على نطاق واسع. ويجب إجراء هذا التشفير بشكل مستقل عن أي تشفير للنقل مثل طبقة مآخذ التوصيل الآمنة SSL. يجب أن تكون جميع ملفات تعريف الارتباط الأخرى معتمة. "انتهاء المهلة" وإنهاء جلسات اتصال النظام بعد فترة متفق عليها بشكل متبادل من عدم النشاط من جانب المستخدم. إنهاء أي جلسات نشطة تم قطعها بسبب انقطاع التيار الكهربائي أو "تعطل" النظام أو حدوث مشكلة في الشبكة أو أي حالة غير معتادة أخرى أو عند قطع الاتصال بواسطة المستخدم. التحقق من صحة جميع المدخلات والمخرجات قبل استخدامها لتجنب الهجمات التي تعتمد على البيانات مثل "البرمجة النصية للمواقع المشتركة" و"حقنة SQL".

10.14 أمان البيانات. نقل جميع معلومات Citi شديدة السرية عبر آلية أخرى غير مستعرض الويب باستخدام خوارزمية تشفير معتمدة من Citi. عندما يلزم تخزين قاعدة البيانات، يجب تخزين جميع معلومات Citi المصنفة على أنها "سرية" أو أعلى في قاعدة بيانات منفصلة (مثل قاعدة بيانات لا تتم مشاركتها مع عملاء المورّدين الآخرين أو لا يمكنهم الوصول إليها).

11.14 الأمان المادي. وضع جميع محطات العمل والخوادم ومعدات الشبكة المستخدمة لتقديم الخدمات بموجب أي عقد في منشآت آمنة مملوكة للمورد أو يقوم المورّد بشغيلها أو يكون متعاقدًا عليها. تقييد الوصول إلى هذه المنشآت الآمنة لموظفي المورّد المعتمدين الذين يحتاجون للوصول لأغراض أداء وظائفهم. مراقبة الوصول إلى هذه المنشآت الآمنة من خلال استخدام حراس الأمن أو كاميرات المراقبة أو أنظمة الدخول المصرح بها أو أي طرق مماثلة بإمكانها تسجيل معلومات الدخول والخروج. الاحتفاظ بجميع وسائط النسخ الاحتياطي والأرشيف التي تحتوي على معلومات Citi أو غيرها من المعلومات المستخدمة لتقديم الخدمات بموجب أي عقد في مناطق تخزين آمنة يتم التحكم فيها بيئيًا وتكون مملوكة للمورد أو يقوم المورّد بشغيلها أو يكون متعاقدًا عليها. تقييد الوصول إلى مناطق تخزين وسائط النسخ الاحتياطي والأرشيف والمحتويات على موظفي المورّدين المعتمدين الذين يحتاجون للوصول لأغراض أداء وظائفهم.

12.14 التعليمات البرمجية الضارة والحماية من الفيروسات. استخدام أحدث منتجات الحماية المتاحة تجاريًا للحماية من الفيروسات والشفرات الضارة على جميع محطات العمل والخوادم المستخدمة لتقديم الخدمات بموجب أي عقد. الإبلاغ عن جميع حالات الإصابة بالفيروسات والشفرات الضارة التي لم يتم التعامل معها من خلال إجراءات الكشف والحماية المنتشرة على أي محطة عمل أو خادم يستخدم لتقديم الخدمات بموجب أي عقد إلى Citi في غضون 24 ساعة من اكتشافها.

13.14 استمرارية الأعمال والتعافي. عمل نسخ احتياطية لجميع الأنظمة والتطبيقات والبيانات المستخدمة لتقديم الخدمات بموجب أي عقد بطريقة تتفق مع إجراءات استئناف الأعمال المحددة في أي مكان آخر في أي عقد.

14.14 معايير مستوى الخدمة الإقليمية. كل منطقة مسؤولة عن حل الشكاوى/المشاكل والرد عليها في الوقت المناسب. يُرجى الاطلاع على المعايير/الإجراءات الإقليمية التي تشمل تنفيذ وتعريف معايير مستوى الخدمة. ستقوم الشركات المغطاة بإجراء الحسابات في التوقيت المناسب ضمن تواريخ البدء التالية:

أ. بالنسبة للتفاعلات الهاتفية والشخصية، يبدأ معيار مستوى الخدمة من تاريخ استقبال المؤسسة للشكوى/المشكلة.

ب. بالنسبة للمراسلات الكتابية والإلكترونية ووسائل التواصل الاجتماعي، يبدأ معيار مستوى الخدمة من تاريخ تحديد عدم الرضا.

15.14 تسجيل المكالمات والاحتفاظ بها. يجب على المورّدين وضع إجراءات لتسجيل وتخزين جميع المكالمات المتعلقة بالشكاوى/المشاكل التي يتم التعامل معها في مراكز الاتصال من قبل الموظفين ومديريهم المباشرين والذين يتمثل دورهم الأساسي في التحدث مع المستهلكين، وذلك لمدة 12 شهرًا على الأقل من تاريخ المكالمة ما لم تقتضي المتطلبات التنظيمية المحلية خلاف ذلك. نقل وسائط النسخ الاحتياطي بشكل دوري إلى منشأة تخزين آمنة خارج الموقع.

15 استمرارية الأعمال

تسري على المورّدين المدرجين في خطة التعافي لوحدة أعمال Citi أو إذا كان المورّد يستضيف تطبيقًا له إمكانات التعافي (مثل القدرة على استعادة التكنولوجيا الرقمية (TRTC))، والتي تستخدمها Citi. يتحمل مسؤول النشاط التجاري (BAO) مسؤولية توضيح قابلية التطبيق ومتطلبات استمرارية الأعمال (COB) للمورّد.

1.15 موارد الاسترداد. يجب أن توفر خطة التعافي من الكوارث الخاصة بالمورّدين موارد بديلة قادرة على تقديم جميع المنتجات والخدمات إلى Citi في حالة تعطيل المواقع الرئيسية للمورد. يجب أن تكون موارد الاسترداد موجودة في مواقع منفصلة جغرافيًا عن المواقع الأساسية مع فصل كافٍ لتقليل، أو القضاء على، التهديد المتمثل في احتمالية أن يؤثر حدث الكارثة نفسه على كل من المواقع الأساسية ومواقع الاسترداد سويًا (في حالة موردي تطبيقات SaaS التي تتم استضافتها لدى موفري الخدمات السحابية (CSP)، فإن هذا الفصل الجغرافي يتطلب مناطق منفصلة لدى موفري الخدمات السحابية (CSP) لكل من البيئة الأولية وبيئة استمرارية الأعمال CoB). ولا تقتصر موارد الاسترداد على نظم المعلومات، بل تشمل جميع الموارد اللازمة لاستمرار تقديم المنتجات والخدمات إلى Citi ويمكن أن تشمل الموظفين والمباني ومعدات الأعمال ومراكز البيانات وشبكات البيانات والصوت وخدمات النقل.

2.15 مستويات الخدمة المتعلقة بالاسترداد. يجب أن تلبي خطة استمرارية الأعمال الخاصة بالمورّدين مستويات الخدمة المحددة بحيث تكون فعالة بالنسبة لشركة Citi. المورّد الذي يستضيف تطبيقات الامتياز الحرجة (FCA) لدى Citi المستخدمة في معالجة المعاملات الحرجة يجب أن يكون لديه إجراء انقطاع الاتصال (Air-Gap) لنسخ البيانات الحرجة المطلوبة للتعافي احتياطيًا بحيث تكون البيانات المنسوخة احتياطيًا غير قابلة للتغيير و/أو مخزنة أثناء انقطاع الاتصال (الانفصال عن الشبكة)، وبحيث يمكن تحقيق استعادة البيانات في نطاق القدرة الزمنية للتعافي التكنولوجي (TRTC).كحد أدنى، يجب أن تحدد خطة التعافي من الكوارث الخاصة بالمورّد قيمًا محددة لكلٍ من:

أ. هدف وقت الاسترداد؛

ب. وهدف نقطة الاسترداد؛

ج. وقدرة الاسترداد؛

د. ومدة الاسترداد.

3.15 خطة التعافي من الكوارث. تُلزم سياسة استمرارية الأعمال لدى Citi المورّدين المُدرجين في خطة تعافي أعمال Citi بأن تكون لديهم خطة للتعافي من الكوارث للمساعدة في ضمان مواصلة شركة Citi في تلقي الخدمات من مواقع بديلة أو بواسطة موظفين بدلاء في موعد لا يتجاوز "هدف وقت الاسترداد" المعمول به. ويتعيّن على المورّدين التشاور مع جهة الاتصال الرئيسية للأعمال المعمول بها في Citi لفهم إذا ما كان يتعين أن يكون لديهم خطة تعافي من الكوارث وأيٌّ من متطلبات Citi يمكن تطبيقها على خطة التعافي من الكوارث، بما في ذلك تلك المتعلقة بأهداف وقت الاسترداد التي، إذا لم يُذكر خلافًا لذلك في العقد المعمول به، تبلغ 4 ساعات أو أقل بالنسبة لتلك العمليات التي صنفتها شركة Citi بدرجة أهمية تبلغ "1"، و24 ساعة أو أقل لتلك العمليات التي صنفتها شركة Citi بدرجة أهمية تبلغ "2"، و72 ساعة أو أقل لتلك العمليات التي صنفتها شركة Citi بدرجة أهمية تبلغ "3". يقدم المورّد نسخة باللغة الإنجليزية من خطة التعافي من الكوارث إلى Citi في غضون عشرة (10) أيام تقويمية من تاريخ سريان الاتفاقية التي ينشأ بموجبها التزام المورّد بالامتثال لمتطلبات القسم 14 هذا، وبصفة سنوية بعد ذلك، إلى جانب دليل على اختباراته الحالية والدورية (إذا طلبت Citi ذلك).

4.15 استدعاء خطة التعافي من الكوارث والإخطار بالأزمات. يقوم المورّد على الفور بإخطار جهة الاتصال الرئيسية للأعمال في Citi:

أ. عندما يستدعي المورّد خطة التعافي من الكوارث الخاصة به؛

ب. بشأن أي أزمة أو تهديد أو تحذير أو حدث إلكتروني ضد المورّد أو مقاوليه من الباطن بحيث يُحتمل إلى حد معقول أن يكون له تأثير سلبي على الخدمات أو المنتجات المُقدمة إلى شركة Citi.

5.15 الاختبارات. يجب اختبار جميع موارد وخطط الاسترداد الخاصة بالمورّد بشكل سنوي على الأقل. ويجب أن تبين الاختبارات قدرة المورّد على الوفاء بمستويات الخدمة المتعلقة بالاسترداد لجميع المنتجات والخدمات المقدمة إلى Citi. يجب أن تكون هذه الاختبارات شاملة وتتضمن النطاق الكامل للخدمات المقدمة إلى Citi. بالإضافة إلى ذلك، يجب أن يشمل الاختبار في نطاقه كل من الأحداث الطبيعية والتي من صنع الإنسان، جنبًا إلى جنب مع الهجمات الإلكترونية بما في ذلك، على سبيل المثال لا الحصر، هجمات حجب الخدمة والهجمات الموزعة لحجب الخدمة وهجمات البرامج الضارة وبرامج الفدية. يجب أن يرسل المورّد إلى Citi إخطارًا مقدمًا قبل 30 يومًا تقويميًا على الأقل من إجراء الاختبار الخاص باسترداد الخدمات المقدمة إلى Citi. ويجوز لشركة Citi المشاركة في اختبار الاسترداد الخاص بالمورّد أو الإشراف عليه. إذا رغبت Citi في المشاركة، فسيقوم المورّد بتزويد Citi بأهداف الاختبار وخطة الاختبار وإجراءات الاتصال بموقع الاختبار قبل أداء الاختبار. في غضون عشرة (10) أيام عمل بعد الانتهاء من كل اختبار، سوف يقدم المورّد إلى Citi ملخصًا لأهداف الاختبار وخطة الاختبار ونتائج الاختبار، بما في ذلك الأطر الزمنية المطلوبة لاستعادة وظائف الأعمال الهامة والأدلة على نتائج الاختبار (مثل لقطات الشاشة).

6.15 يجب على المورّدين اختبار سيناريوهات التعطل التالية:

أ. حجب الوصول (DOA)

ب. حجب الخدمة (DOS)

7.15 مشاركة شركة Citi في اختبار المورّد ومراجعتها له. بالنسبة لأي اختبار (بما في ذلك إعادة الاختبار) من قبل المورّد لخطة التعافي من الكوارث، ستشارك Citi في نشاط يتناسب مع خطورة العملية/هدف وقت الاسترداد (RTO).

8.15 لاختبارات حجب الوصول (DOA):

أ. العمليات الأكثر أهمية لامتياز Citi. سوف تشارك شركة Citi في نشاط اختبارات المورّد لكل العمليات التي تعرّفها باعتبارها "بالغة الأهمية للامتياز" أو تشرف عليها. وبالنسبة لهذه العمليات، يسمح المورّد لشركة Citi بمراجعة خطط التعافي التي تغطي الأعمال التجارية و/أو التقنية (حسب الاقتضاء)، ونصوص الاختبار، ونتائج الاختبار، والأدلة.

ب. العمليات مع هدف وقت استرداد أقل من مدة 24 ساعة أو يساويها. ما لم تطلب شركة Citi خلافًا لذلك، فإنها ليست بحاجة للمشاركة في نشاط اختبارات المورّد أو الإشراف عليها، ولكنها ستراجع خطط التعافي التي تغطي الأعمال التجارية و/أو التقنية (حسب الاقتضاء)، ونصوص الاختبار، ونتائج الاختبار، والأدلة.

ج. العمليات حيث يكون هدف وقت الاسترداد (RTO) أقل من 24 ساعة. ما لم تطلب شركة Citi خلافًا لذلك، فإنها ستلزم المورّد بالتعهد بخطط التعافي التي تغطي الأعمال التجارية و/أو التقنية (حسب الاقتضاء)، ونصوص الاختبار، ونتائج الاختبار، والأدلة.

9.15 لاختبارات حجب الخدمة (DOS):

أ. العمليات مع هدف وقت استرداد أقل من مدة 72 ساعة أو يساويها. سوف تشارك شركة Citi في نشاط اختبارات المورّد لكل التطبيقات. يسمح المورّد لشركة Citi بمراجعة خطط التعافي التي تغطي التكنولوجيا، ونصوص الاختبار، ونتائج الاختبار، والأدلة.

ب. العمليات مع هدف وقت استرداد يتجاوز مدة 72 ساعة. ما لم تطلب شركة Citi خلافًا لذلك، فإنها ستلزم المورّد بالتعهد بخطط التعافي التي تغطي الأعمال التجارية و/أو التقنية (حسب الاقتضاء)، ونصوص الاختبار، ونتائج الاختبار، والأدلة.

10.15 معالجة نتائج الاختبار. إذا أظهرت أيٌ من نتائج اختبارات المورّد فشلاً في تحقيق أي هدف من أهداف الاختبار أو أي هدف من أهداف وقت الاسترداد المعمول بها، سيتعهد المورّد بتنفيذ تحليل لسبب المصدر ولمعالجة أي قصور يتم تحديده فورًا. بعد تنفيذ هذه المعالجة، يعيد المورّد الاختبار في موعد أقصاه مائة وعشرين (120) يومًا تقويميًا بعد فشل الاختبار الأولي (أو الفترة الزمنية المُحددة في أمر العمل ذي الصلة).

11.15 اختبار الحجم. يجب على المورّد الذي يستضيف تطبيقات الامتياز الحرجة (FCA) لدى Citi المستخدمة في معالجة المعاملات الحرجة أن يثبت أنه يمكنه معالجة أحجام الإنتاج في بيئة استمرارية الأعمال/التعافي من الكوارث. يجب أن تتفق شركة Citi والمورّد على المنهجية المفترض استخدامها لإجراء عملية التحقق.

12.15 إدارة الأزمات. يجب أن يحتفظ المورّد، بجانب خطة استمرارية الأعمال، بخطة لإدارة الأزمات من أجل الإشراف على عمليات الاسترداد والسيطرة عليها. وعلى أقل تقدير، يجب أن تحدد خطة المورّد لإدارة الأزمات أشخاصًا محددين يتمتعون بالسلطة الكافية لتفعيل عملية الاسترداد، وتحديد بروتوكولات الاتصال والتصعيد لجمع المعلومات المتعلقة بالأزمات ونشرها، وتضمين بروتوكولات الإخطار والتصعيد للتواصل مع Citi في حالة وقوع أزمة.

13.15 التقييمات. يخضع الموردون لعملية تقييم استمرارية أعمال الأطراف الثالثة لدى Citi وذلك من أجل تقييم قدرات استمرارية الأعمال بما يتناسب مع مدى أهمية العملية/ هدف وقت استرداد (RTO):

أ. يجب تقييم الموردين الذين يدعمون العمليات مع هدف وقت استرداد أقل من مدة 24 ساعة أو يساويها سنويًا

ب. يجب إجراء تقييمات المورّدين الذين يدعمون عمليات الامتياز الحرجة في موقع المورّد

ج. لا يتعين على الموردين الذي يدعمون العمليات مع هدف وقت استرداد يتجاوز مدة 24 ساعة وأقل من مدة 72 ساعة أو يساويها إجراء تقييم ولكن يجب عليهم إثبات قدراتهم على التعافي سنويًا

د. وسيتألف التقييم من استبيانات تعافي الأعمال التي تتطلب إجابات من المورّد إضافةً إلى الأدلة. وإذا ما كشفت النتائج التي توصل إليها تقييم استمرارية الأعمال (CoB) عن وجود مشكلات أو مخاوف، فستحرص Citi على توثيق النتائج في إخطار يتم تقديمه إلى المورّد كما ستعمل مع المورّد لتحديد الوسائل اللازمة لتصحيح المشكلات.

14.15 التغييرات في خطة التعافي من الكوارث. يجوز أن يقوم المورّد بتغيير خطة التعافي من الكوارث الخاصة به طالما أن التغييرات لا تؤدي إلى تدهور خطة التعافي من الكوارث بطريقة من المحتمل أن تؤثر سلبًا على الخدمات (مثل إطالة أهداف وقت الاسترداد الخاصة بها RTO). يلتزم المورّد بأن يقوم بإبلاغ Citi على الفور بأي تغييرات تطرأ على خطة التعافي من الكوارث، ويقوم، بناءً على طلب Citi، بشرح التغييرات حتى يتفهم العميل التغييرات تمامًا ويكون قادرًا على الاستجابة لها.

15.15 خطة التعافي من الكوارث للمقاولين من الباطن. يلتزم المورّد بأن يضمن أن يكون لدى أي مقاول من الباطن تابع للمورد خطة للتعافي من الكوارث تتوافق تمامًا مع متطلبات Citi حيال المورّدين.

16.15 استخدام أنظمة Citi لتقديم الخدمات. بناء على طلب Citi أو الشركات التابعة لـ Citi، فسوق يشارك المورّدون الذين يستخدمون أنظمة Citi في تدريبات التعافي من الكوارث التي تجريها Citi بدون تكلفة أو رسوم من Citi.

17.15 متطلبات خطة التعافي من الكوارث المطبقة على الخدمات المستضافة. إلى حد قيام المورّد بإدارة وتوفير خدمة مستضافة لـ Citi، يجب أن تطبق كذلك الأحكام التالية. سوف تتضمن خطة التعافي من الكوارث على الأقل ما يلي:

أ. إجراءات النسخ الاحتياطي/استعادة تشغيل الخدمات المستضافة وتطبيقها، بما في ذلك خطة مفصلة وموثقة للاستجابة للانقطاع المطول في الخدمات الناتج عن انقطاع التيار الكهربائي أو تعطل النظام أو الكوارث الطبيعية أو غيرها من الظروف غير المتوقعة التي تتضمن عمليات وإجراءات خاصة باستئناف العمليات في غضون فترة زمنية يتفق عليها الطرفان؛

ب. وإجراءات حماية جميع المحتوى؛

ج. والإجراءات وأي اتفاقيات مع طرف ثالث لاستبدال المعدات (مثل أجهزة الكمبيوتر)،

د. والإجراءات الخاصة بأي منشآت إنتاج خارج الموقع.

ه. وإضافةً لذلك، ستنص خطة التعافي من الكوارث الخاصة بالمورّد على ما يلي: (أ) أن يخطر المورّد Citi كتابيًا في غضون ساعتين (2) من أي كارثة يمكن أن تؤثر سلبًا على الخدمات المستضافة؛ (ب) أن يقدم المورّد لشركة Citi، في غضون 24 ساعة من الإشعار المذكور، خطة لمواصلة تقديم الخدمات المستضافة في منشأة معالجة بديلة، (ج) وجوب معاودة الخدمات المستضافة للعمل بشكل كامل في غضون 48 ساعة من الإشعار الأولي.

و. يوافق المورّد، عند الطلب، على إصدار المعلومات اللازمة التي تتيح لـ Citi تطوير خطة التعافي من الكوارث وخطة استمرارية الأعمال والتي ستعمل بالتنسيق مع خطة التعافي من الكوارث الخاصة بالمورّد وخطة استمرارية الأعمال.

ز. في حالة تعطل أجزاء من منشآت المورّد، سيعامل المورّد Citi على نحو لا يقل تفضيلًا عن معاملة المورّد لعملائه التجاريين الآخرين.

18.15 المرونة التشغيلية. يجب على المورّد التأكد من أن أي انقطاع في تقديم عناصر الخدمات التي تصل إلى مستوى خدمات الأعمال المهمة/الحرجة أو تدعم تقديم Citi لخدمات الأعمال المهمة/الحرجة، على النحو الذي تحدده Citi من وقت لآخر (يُشار إليها باسم "خدمات الأعمال المهمة/الحرجة ") لا يتجاوز المدة التي حددتها Citi أو يخالف أي مقياس ذي صلة تحدده Citi (ويُشار إليها باسم "درجات تحمل الأثر") حسبما يتم إخطار المورّد به من وقت لآخر.

أ. سيتم التعبير عن "درجات تحمل الأثر" كمقياس واضح، بما في ذلك الحد الأقصى للمدة التي يمكن تحملها أو الحد الأقصى لوقت التوقف الذي يمكن تحمله والذي قد يتعطل فيه تسليم خدمة الأعمال المهمة/الحرجة. يتعين على Citi والمورّد مراجعة "درجات تحمل الأثر" سنويًا كجزء من عمليات حوكمة العقود المستمرة. عندما يُطلب من Citi تعيين "درجتين لتحمل الأثر" لخدمة الأعمال المهمة/الحرجة الفردية نظرًا لمتطلبات أكثر من هيئة تنظيمية واحدة، فقد تحدد Citi "درجات تحمل أثر" منفصلة لخدمة الأعمال المهمة/الحرجة هذه. يجب على المورّد:

ب. إخطار Citi بمجرد أن يصل إلى علمها أنها فشلت (أو من المحتمل بشكل معقول أن تفشل) في تقديم أي خدمة أعمال مهمة/حرجة ضمن نطاق (درجة/درجات تحمل الأثر) المقابل الذي حددته Citi جنبًا إلى جنب مع شرح لأسباب أي فشل محتمل أو فشل فعلي والخطوات التي يتم اتخاذها للتخفيف من أثر ذلك الفشل؛

ج. عند الطلب، تقديم مساعدة معقولة إلى Citi لتمكينها من تحديد الأشخاص والعمليات والتكنولوجيا والمرافق والمعلومات اللازمة للمورد لتقديم أي خدمات أعمال مهمة/حرجة؛

د. تقديم مساعدة معقولة إلى Citi لأغراض تمكين Citi لتأدية ما يلي:

1. أي اختبار سيناريو داخلي لقدرة المورّد على البقاء ضمن نطاق (درجة/درجات تحمل الأثر) لكل خدمة أعمال مهمة/حرجة في حالة حدوث اضطراب شديد ولكنه معقول في عمليات Citi أو عمليات المورّد؛
2. وأي دروس مستفادة يتم ممارستها بعد اختبار السيناريو لتمكين Citi من تحديد نقاط الضعف وأي إجراءات ضرورية لتحسين قدرة المورّد على الاستجابة بفعالية والتعافي من الاضطرابات المستقبلية.

ه. عندما يحدد أي اختبار سيناريو داخلي من قبل Citi نقاط الضعف أو القيود المفروضة على قدرة المورّد على تقديم خدمات الأعمال المهمة/الحاسمة ضمن التسامح مع التأثير المقابل الذي حددته Citi وبعد أي فشل من جانب المورّد في تقديم أي خدمة أعمال مهمة/حرجة ضمن نطاق (درجة/درجات تحمل الأثر) المقابل الذي حددته Citi، يوافق الطرفان على خطة (بما في ذلك جدول زمني لتنفيذ الخطة) لضمان أن يتخذ المورّد الخطوات اللازمة لحل أو التخفيف من نقاط الضعف أو القيود أو معالجة سبب الفشل في البقاء ضمن نطاق (درجة/درجات تحمل الأثر) (حسب الاقتضاء) في أقرب وقت ممكن عمليًا.

16 المعايير العالمية لفحص الخلفية الأمنية

تسري على المورّدين الذين يتمتع موظفوهم بإمكانية الوصول إلى أنظمة/شبكات Citi و/أو الوصول دون مرافقة إلى مقرات Citi. (يجب حصول هؤلاء الموظفين على رقم تعريف الموظف العالمي (GEID)، وأن يكونوا مسجلين في نظام الإدارة المعنى بغير الموظفين)

1.16 نظرة عامة - فحص الخلفية الأمنية. يجب إجراء فحص الخلفية الأمنية وفقًا لجميع القوانين واللوائح المحلية المعمول بها. ويجب تقديم جميع المعلومات والإفصاحات الذاتية المبينة ضمن هذه الوثيقة بواسطة موظفي المورّد حسب الاقتضاء. وقد يُشكل تزييف المعلومات أو إغفالها سواءٌ في السيرة الذاتية أو أثناء المقابلة الشخصية أو في أيٍ من نماذج الالتحاق بالعمل أو أثناء عملية الالتحاق بالعمل، بصرف النظر عن وقت اكتشاف ذلك التزييف أو الإغفال، سببًا لرفض أو إنهاء التكليف لدى Citi وفقًا للقانون المحلي. وقد تُشكل أيضًا النتائج السلبية لأي عملية فحص يتم إجراؤها، بصرف النظر عن وقت اكتشافها، سببًا لرفض أو إنهاء التكليف لدى Citi وفقًا للقانون المحلي.

يمكن الاطلاع على معلومات إضافية حول توقيت إتمام فحص الخلفية الأمنية والمتطلبات والاستثناءات الخاصة بكل دولة فيما يتعلق بهذه المعايير
على هذا الرابط
https://www.citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.

2.16 جمع المعلومات الأساسية والتحقق من الهوية. قبل أن يبدأ أي موظف من موظفي المورّد في القيام بأي مهمة لدى Citi، يجب على المورّدين جمع الاسمين الأول والأخير للموظف والعنوان البريدي والعنوان الدائم (إذا كان مختلفًا) ورقم الهاتف وعنوان البريد الإلكتروني (إن وُجِد). كما يجب على موظفي المُورّد تقديم وثائق تثبت هُويتهم. وقد يتضمن ذلك تقديم معلومات و/أو وثائق خاصة برقم الهُوية الوطنية أو بطاقة هُوية صادرة عن الحكومة ملصق بها صورة شخصية أو جواز سفر.

3.16 فحص العقوبات. يجب فحص جميع موظفي المورّد في ضوء قائمة المواطنين المرصودين لاعتبارات خاصة والأشخاص المحظورين (يُشار إليهم باسم "SDN") الصادرة عن مكتب مراقبة الأصول الأجنبية (يُشار إليها باسم "OFAC") التابع لوزارة الخزانة الأمريكية وقائمة المناطق والاختصاصات القضائية الخاضعة لعقوبات مفروضة عليها من جانب الولايات المتحدة (يُشار إليها باسم "العقوبات الأمريكية"). ويجب أن يُطبق الفحص على الأسماء والعناوين والأسماء المستعارة وتاريخ الميلاد المستمد من عملية التحقق، قبل يومهم الأول من التكليف (باستثناء الحالات التي لا يسمح بها القانون المحلي). ويحظر على موظفي المورّد الذين تتطابق أسماؤهم إيجابياً مع قيد وارد في قائمة العقوبات العمل في التكليف لدى Citi. إذ قد تسفر أي إشارة أو تحريف عن انعدام الأهلية لإنجاز التكليف أو إغلاقه.

تتوفر القوائم الصادرة عن مكتب مراقبة الأصول الأجنبية (يُشار إليها باسم "OFAC") لعامة الجمهور في هذا الموقع الإلكتروني: https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

4.16 الامتثال لقوانين الهجرة. يجب على المُورّد إثبات تبنيه لمجموعة من البروتوكولات للتحقق من أن موظفيه مصرح لهم بالعمل في البلدان المكلفين بالعمل فيها، وكذلك امتثاله لجميع القوانين واللوائح المعمول بها للتحقق من أهلية التوظيف. ويجب على المُورّد أيضًا إثبات تبنيه لمجموعة من البروتوكولات لضمان أن موظفيه يمتثلون بخلاف ذلك لجميع قوانين ولوائح الهجرة المعمول بها وأنهم يحملون تصنيف التأشيرة المناسب الذي يمكنهم من إجراء المهام والأنشطة التي يضطلعون بها.

5.16 السجل الوظيفي. يجب على المُوردين التحقق من السجل الوظيفي لموظفيهم على مدار السبع (7) أو العشر (10) سنواتٍ الماضية إذا لزم الأمر وفقًا للنظم واللوائح. يجب التحقق من السجل الوظيفي لأي موظف لضمان أنه تم تمثيل أصحاب العمل والمناصب والتواريخ والواجبات على نحو دقيق. يجب على موظفي المُورّد أيضًا الإفصاح عن أي عمل أو مهمة كُلِّفوا بأدائها بصفتهم يحملون منصب مستشارًا أو عاملاً مؤقتًا لدى Citi أو أي من شركاتها السابقة (بما في ذلك، على سبيل المثال لا الحصر: Citibank و/أو Citicorp و/أو Travelers و/أو Salomon Brothers و/أو SmithBarney). ويجب عليهم أيضًا الإفصاح عما إذا كان قد تم إنهاء توظيفهم أو تكليفهم أو طُلب منهم الاستقالة منه أو تم رفضه بعد تلقي عرضٍ من Citi أو أي من شركاتها السابقة.

6.16 السجل التعليمي. يجب على المُورّدين أن يتحققوا من حصول موظفيهم على أعلى مستويات التعليم. وينبغي أن تتضمن المعلومات المتحقق من صحتها تواريخ الحضور واسم (أسماء) المؤسسات التعليمية، والعنوان (العناوين) والدرجة (الدرجات) التي تم الحصول عليها.

7.16 الخلفية الجنائية. حيثما يكون مسموحًا بذلك قانونًا، يجب على أي موظف أو مقاول من الباطن تابع للمورّد أن يفصح لشركة Citiإذا ما تعرض للاعتقال أو الاستدعاء أو المثول أو الاتهام أو الإدانة في أي جريمة جنائية، بما في ذلك الإقرار بالذنب أو عدم الإقرار به مع عدم الدفع بالاعتراض، وأي مشاركة في برنامج تغيير مسار العقوبة قبل المحاكمة أو أي برنامج مماثل. ويجب إتمام المراجعة الإدارية للسجلات الجنائية و/أو عمليات التحقق من بصمات الأصابع قبل تاريخ بدء التكليف حيثما يكن ذلك مسموحًا به ومتاحًا من الناحية القانونية. قد تؤدي الإدانات الجنائية في جرائم تتعلق بالسرقة أو الاحتيال أو الغش أو خيانة الأمانة، إلا في الحالات التي يحظرها القانون، إلى رفض و/أو انعدام الأهلية للعمل مع Citi. وقد تؤدي الإدانات الأخرى إلى رفض و/أو انعدام الأهلية للتكليف استنادًا إلى القوانين واللوائح المحلية المعمول بها.

8.16 فحص تعاطي المخدرات. حينما يُسمح بذلك قانونًا، يجب أن يضمن المورّدون إتمام موظفيهم لفحص تعاطي المخدرات قبل بدء التكليف لدى Citi. وعلى أقل تقدير، يجب أن يكون فحص تعاطي المخدرات عبارة عن اختبار من "5 شرائح"، يختبر وجود مواد الأمفيتامين وكانابينويد (رباعي هيدرو كانابينول) والكوكايين والأفيون والفنسيكليدين. وتكون النتائج الإيجابية قاطعة وكافية لرفض التكليف، سواءً تم تلقي النتائج قبل بدء العمل أو بعده وذلك باستثناء الحالات التي لا يسمح بها القانون المحلي. ويجوز أن يُطلب من بعض موظفي المورّد استيفاء اختبار فحص تعاطي المخدرات أثناء تكليفهم نظرًا لما تقتضيه متطلبات الوظيفة (مثل السائقين والطيارين) أو لأسباب أخرى وفقًا للقوانين واللوائح المحلية.

9.16 إعادة الفحص. يجب إعادة فحص موظفي المورّدين الذين يتم إنهاء تكليفهم في حالة إعادة تكليفهم بمهام جديدة لدى Citi. وللاطلاع على مزيد من المعلومات عن متطلبات إعادة الفحص، يُرجى الرجوع إلى المتطلبات والاستثناءات الخاصة بكل دولة موجودة على الرابط https://citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.

10.16 الانتقالات الدولية. يجب إتمام جميع عمليات الفحص وفقًا للوائح البلد الذي يكون فيه التكليف. إذا انتقل أيٌ من موظفي المورّد إلى بلدٍ جديد وانقطع عن العمل لدى Citi، فيجب إعادة فحص هذا الموظف وفقًا لمتطلبات البلد الجديد.

17 النفقات

المورّدون المؤهلون حسب التعاقدات للمطالبة بنفقات أعمال واجبة السداد.

1.17 نظرة عامة. لن تسدد Citi سوى النفقات المعقولة المتعلقة بالأعمال والتي اعتمدتها مسبقًا بشكل كتابي وتكبدها المورّد فيما يتعلق بتقديم المنتجات والخدمات إليها ووفقًا لشروط العقد المعمول به أو سياسة Citi لإدارة النفقات، حسب الاقتضاء، ويتم إثباتها بشكلٍ كافٍ بالإيصالات أو الفواتير أو جداول رحلات السفر أو غيرها من أشكال الوثائق التي تعتبرها Citi مقبولة.

2.17 استرداد التكاليف. يجب توثيق هذه النفقات وإصدار فواتير بها إلى Citi وفقًا لمتطلبات نظام إعداد الفواتير لدى Citi. لا يجب أن يتحمل أي موظف من موظفي Citi نفقات المورّد نيابةً عن المورّد. ويجب أن تتضمن أي نفقات تُرسل إلى Citi بشأن سداد أي من عناصر النفقات الصالحة والمعتمدة (إضافة إلى جميع متطلبات الفوترة الأخرى) ما يلي:

أ. الغرض التجاري من النفقات؛
ب. قيمة النفقات ووصفها؛
ج. مكان وتاريخ النفقات؛
د. اسم/وصف المشروع الذي يقدم المورّد الخدمات فيما يتعلق به؛
ه. وأسماء وعلاقة العمل الخاصة بممثل Citi الذي طلب الحصول على الخدمة (الخدمات) التي نشأت النفقات بشأنها؛
و. رقم أمر الشراء، عند الاقتضاء.

للاطلاع على معلومات بشأن النفقات التجارية القابلة للسداد والمسموح بها، يُرجى التواصل مع جهة الاتصال الرئيسية للأعمال في Citi. يجب إرسال الإيصالات أو الفواتير أو جداول رحلات السفر أو غيرها من أشكال الوثائق الداعمة التي تعتبرها شركة Citi مقبولة مع مطالبة السداد. يجب أن تكون مطالبات السداد متوافقة مع الأحكام الواردة في العقد المعمول به أو مع سياسة Citi لإدارة النفقات، حسب الاقتضاء، ويجب كذلك اعتمادها من جانب شركة راعية مناسبة و/أو جهة الاتصال الرئيسية للأعمال في Citi. ولن يتم سداد الطلبات غير المستوفية للمتطلبات.

18 أمان المعلومات (IS)

يسري على المورّدين الذين يمكنهم الوصول إلى/معالجة/تخزين/إدارة كل معلومات Citi حسبما هي مصنفة ومحددة في الملحق) و/أو استضافة تطبيقات الإنترنت التي تحمل علامة Citi التجارية و/أو التي لديها اتصال بموارد شبكة Citi و/أو الذين يحتاجون إلى وصول دون مرافقة إلى مرافق Citi.

1.18 نظرة عامة. يعرض هذا القسم الحد الأدنى من المتطلبات الخاصة بمورّدي Citi الذين يعملون على تخزين معلومات Citi أو معالجتها أو إدارتها أو الوصول إليها و/أو استضافة تطبيقات Citi وذلك فيما يتعلق بضوابط حماية المعلومات التي تتوقعها Citi لضمان أمان المعلومات وفقًا للمتطلبات القانونية والتنظيمية المعمول بها وأعلى معايير الصناعة (مثل ISO/IEC 27002) في المواقع التي تزاول فيها Citi ومورّدوها أعمالهم التجارية. وإذا حددت القوانين أو اللوائح أو المعايير المحلية ذات الصلة في الصناعة معايير أعلى مما هو منصوص عليه في هذه الوثيقة، يجب على المورّدين الامتثال لهذه القوانين أو اللوائح أو المعايير. وإضافة إلى ذلك، قد يُطلب من المورّدين تضمين ممارسات وإجراءات إضافية فيما يتعلق بأمن المعلومات كجزء من امتثالهم لسياسات Citi والشروط والأحكام المنصوص عليها في أي عقد. إذا قرر أي من المورّدين تنفيذ ممارسات أمنية إضافية أو إجراءات مفصلة فيما يتعلق بأمان المعلومات، يجب على المورّد التأكد من أن هذه الممارسات والإجراءات لا تتعارض مع الحد الأدنى من الضوابط المحددة في هذا القسم.

2.18 سياسة وحوكمة أمان المعلومات. يجب أن يكون لدى المورّدين سياسات ومعايير موثقة خاصة بأمان المعلومات. يجب أن تتضمن حوكمة السياسة أدوارًا ومسؤوليات محددة، ومراجعةً سنوية، وتحديثًا للسياسات والمعايير، لتكون متوافقة مع حالة التكنولوجيا، ومعايير الصناعة، والمتطلبات القانونية والتنظيمية.

3.18 الفصل بين الواجبات. يجب أن ينفّذ المورّد العمليات بما يضمن عدم قيام أي فرد واحد بوظيفتين من وظائف الأعمال أو وظيفتين من وظائف تكنولوجيا المعلومات أو وظيفتين من وظائف نظام المعلومات الخاضعة للرقابة من خلال الوصول المستمر لنفس النشاط أو التغيير أو نظام المعلومات أو المعاملة دون إذن أو دون اكتشافه ما لم تتوفر ضوابط تعويضية كافية لتخفيف المخاطر.

4.18 استثناءات.

أ. يجوز للمستخدم البدء في، أو الموافقة على، معاملة حقيقية وأيضًا مشاركته في اختبار المتطلبات الجديدة لنفس نظام معلومات Citi في بيئة غير إنتاجية.

ب. يجوز للمستخدم الذي يتقلد وظيفة تطوير أن يوفر الدعم للإنتاج، ولكن لا يمكن منحه الوصول المستمر إلى نظام معلومات Citi إلا إذا كان الوصول يقتصر على القراءة أو العرض فقط ولا يشمل الوصول إلى المعلومات السرية أو العليا.

ج. يجب على الشخص الذي يتقلد وظيفة تطوير أو تصديق ويحتاج إلى تقديم دعم التركيب/الإصلاح بالاستفادة من وظيفة التنفيذ استخدام الوصول المؤقت المُميز إلى نظام المعلومات الخاضع للسيطرة.

د. يجب على الشخص الذي يحتاج إلى تحديث بيانات الإنتاج خارج عناصر التحكم في التطبيق استخدام الوصول المؤقت المُميز.

ه. يجب على الشخص الذي يحتاج إلى الاطلاع على بيانات تحتوي على معلومات تعريف شخصية سرية أو بيانات معلومات تعريف شخصية حساسة خارج ضوابط التطبيق استخدام الوصول المؤقت المُميز.

و. يُحظر على الأفراد الذين ينفذون وظيفة تطوير أو تصديق تعديل نظام التشغيل أو برنامج البنية الأساسية لقاعدة البيانات أو تثبيتها في أنظمة المعلومات الخاضعة للرقابة.

5.18 التزام الإدارة بأمان المعلومات. يخضع المورّدون، الذين سيستضيفون أحد تطبيقات واجهة الإنترنت التي تحمل العلامة التجارية لشركة Citi و/أو الذين تم السماح لهم بالوصول إلى معلومات Citi المُصنفة باعتبارها سرية أو عليا، لعملية تقييم لأمان المعلومات من طرف خارجي (TPISA) لصالح شركة Citi لتقييم سياسات المورّدين وإجراءاتهم وضوابطهم فيما يتعلق بالامتثال لمتطلبات شركة Citi وأي متطلبات قانونية و/أو تنظيمية (منطبقة على Citi أو على المورّد) تتعلق بأمان المعلومات.

وسوف يتألف التقييم من استبيانات أمنية تتطلب إجابات من المورّد مع أدلة ثبوتية وزيارات إلى المواقع حيث يمكن تخزين المعلومات السرية أو العليا الخاصة بشركة Citi أو معالجتها أو إدارتها أو الوصول إليها بواسطة طرف ثالث لتلبية احتياجات أعمال شركة Citi وعملائها. وإذا ما كشفت النتائج التي توصل إليها تقييم TPISA عن وجود مشكلات أو مخاوف أمنية، فستحرص Citi على توثيق النتائج في إخطار يتم تقديمه إلى المورّد كما ستعمل مع المورّد لتحديد الوسائل اللازمة لتصحيح المشكلات. يجب على المورّدين إجراء التصحيحات اللازمة أو ضوابط التعويض الضرورية على وجه السرعة لمعالجة مخاوف شركة Citi بما يرضيها؛ وفي أي حال في غضون 180 يومًا تقويميًا بالنسبة للمشاكل عالية المخاطر، وفي غضون 240 يومًا تقويميًا بالنسبة للمشاكل متوسطة المخاطر، وقبل حلول التقييم التالي بالنسبة للمشاكل منخفضة المخاطر.

أ. يجب على المورّد إجراء تقييمات منتظمة لعملياته التجارية والضوابط ذات الصلة وفقًا لمعايير وسياسات وإجراءات أمان المعلومات. يجب أن تتضمن التقييمات الدورية، كحد أدنى، ما يلي:

1. تقييم العمليات التي يستخدمها المورّد لضمان الامتثال لسياسة ومعايير أمان المعلومات؛
2. تقييم الموارد الداعمة، مثل التطبيقات والبنية الأساسية المستخدمة بواسطة المورّد وعمليات أمان المعلومات التي يستخدمها المقاولون من الباطن التابعين للمورّد (عند الاقتضاء) والتي تدعم عملياتهم التجارية، أو تسمح لشركة Citi بإجراء هذه التقييمات. الامتثال مطلوب في حالة توقيع طرف ثالث على عقد جديد أو تجديده لعقد حالي مع مقاول من الباطن يمكنه الوصول إلى معلومات شركة Citi المُصنّفة باعتبارها سرية أو عليا أو معالجتها أو إدارتها أو التخلص منها.

ب. يجب توثيق المشاكل التي تم تحديدها نتيجةً لأي تقييم لمخاطر أمان المعلومات وتتبعها حتى الإغلاق مع تقديم الأدلة على المعالجة إلى Citi.

ج. إذا تم نقل وظيفة إدارة أمان المعلومات الخاصة بالمورّد عبر حدود الدولة، فيجب على المورّد الحصول على موافقة موثقة من Citi قبل إعادة النقل هذه.

د. إذا استحوذ المورّد على كيانٍ جديد، فيجب على المورّد إتمام تقييم الكيان المستحوذ عليه للامتثال لهذه المعايير.

ه. يجب على المورّد عدم إسناد وظائف الإدارة الأمنية إلى جهات خارجية بما في ذلك، على سبيل المثال لا الحصر، وظائف إدارة برنامج جدار الحماية أو إدارة تكوين الأمان أو إدارة التصحيحات البرمجية أو إدارة أمان المعلومات (ISA) بالنسبة للأنظمة المستخدمة لتخزين و/أو معالجة و/أو نقل معلومات Citi ما لم توافق Citi كتابةً على هذا التعهيد مُقدمًا.

و. إذا كان المورّد يستضيف برنامجًا أو موقعاً إلكترونيًا يحتوي على معلومات Citi أو موسوم بعلامة Citi التجارية، فيجب إجراء تقييمات دورية للمخاطر وفقًا لمعيار اختبار أمان النظام (SST) لدى Citi ويجب معالجة أي قضايا جوهرية يتم تحديدها أثناء التقييم ضمن الأطر الزمنية المُحددة في معيار اختبار أمان النظام (SST) لدى Citi. بالإضافة إلى ذلك، سوف يمتثل المورّد لمعايير إدارة أمان المعلومات ISO / IEC 207000 ذات الصلة (معيار لأمان المعلومات تنشره المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الدولية للتقنيّات الكهربائية (IEC)) (أو معايير إدارة أمان المعلومات اللاحقة التي تضع معايير وبروتوكولات أعلى)؛ ويلتزم بأحكام أمان الكمبيوتر التي يتضمنها القسم 18.

ز. إذا دعت الحاجة إلى الاتصال بالخوادم و/أو نظم المعلومات على الشبكة الداخلية لشركة Citi، يجب على المورّد عندئذ إخطار جهة الاتصال الرئيسية للأعمال في Citi بحيث يمكن اتباع إجراءات الاتصال الحالية.

ح. يجب أن يخطر المورّد بشكل فوري جهة الاتصال المناسبة لدى Citi عن أي وصول غير مصرح به لمعلومات Citi أو الحصول عليها أو فقدانها أو إتلافها أو حذفها أو أي تلاعب آخر بنظم المعلومات المستخدمة لتخزين معلومات Citi و/أو معالجتها و/أو نقلها.

ط. يجب على المورّد ضمان أن تستخدم الأنشطة عالية المخاطر والتغييرات التي تطرأ على البيانات الحساسة

مسارات تدقيق توفر إمكانية تحديد ماهية أي شخص يجري أي نشاط أو يغيّر أي بيانات فضلاً عن تحديد ماهية هذه الأنشطة والبيانات.

ي. يجب على المورّد ضمان إخفاء كافة البيانات الحساسة من الشاشات والأوراق (ويشمل ذلك مثلاً تقارير الرصد والتجاوزات والتقارير التنظيمية وغيرها من التقارير).

ك. يجب على المورّد تقييد طباعة البيانات الحساسة أو تسجيلها أو نسخها، بما في ذلك ما يكون باستخدام "الأجهزة الخاصة" بالمورّد. يجب أن يبذل المورّد كل الجهود المعقولة لإعادة جميع معلومات Citi أو إتلافها في وقت زمني متفق عليه خلال الاتفاقية أو عند انتهائها.

ل. يجب على المورّد أن يتأكد من توقيع طاقم عمل المورّد بأكمله (الموظفون، المقاولون، الموظفون المؤقتون، المقاولون من الباطن) ممن يمكنهم الوصول إلى معلومات Citi اتفاقية عدم الإفصاح (NDA).

م. يجب تزويد موظفي المورّد بدليل الموظف أو وثيقة مماثلة تنطوي على إجراءات التأديب في حال انتهاك أو عدم الامتثال لمدونة قواعد السلوك لدى المورّد وسياسات الموارد البشرية التي يجب الإقرار بها باعتبارها جزءًا من عملية التوظيف.

ن. يجب أن يكون لدى المورّد إجراءات قائمة واجب اتباعها لاسترداد كل الأصول عندما يتم إنهاء عمل أي شخص سواء كان موظفًا أو غير موظف أو عند استقالته.

6.18 المخاطر المتعلقة بأمان معلومات المقاولين من الباطن. يجب على المورّد أن يلزم المتعهدين من الباطن الذين يمكنهم الوصول إلى بيانات عملائهم بأن يطلبوا تقييمات أمان المعلومات (IS) قبل إبرام العقود أو بعد إبرام العقود الدورية ويقوم بتنفيذها موظفو أمان المعلومات المؤهلون وتشمل:

أ. عملية تقييم أمان معلومات المقاولين من الباطن معتمدة من الإدارة وهي نافذة وتغطي جميع الخطوات بدايةً من بدء التقييم وحتى إدارة المشاكل.

ب. يضمن المورّدون تنفيذ تقييمات مخاطر أمان المعلومات على المقاولين من الباطن لديهم ممن يمكنهم الوصول إلى بيانات Citi السرية والعليا باستخدام استبيان تقييم أمان المعلومات أو أداة مكافئة تغطي نطاقات أمان المعلومات بما يتوافق مع تلك التي يغطيها استبيان تقييم أمان معلومات الأطراف الثالثة (TPAQ) لدى Citi وتشمل وسيلة منطقية لحساب مخاطر أمان المعلومات فيما يتعلق بالمقاولين من الباطن.

ج. يضمن المورّدون أنهم يقيّمون ضوابط أمان معلومات المقاولين من الباطن الذين يمكنهم الوصول إلى معلومات Citi، وتتبع عمليات استكمال التقييمات، وإدارة المشاكل المذكورة وخطط العمل التصحيحية (CAP) حتى يتم إغلاقها.

7.18 المسؤولية عن الأصول:

أ. يجب على المورّد التأكد من الاحتفاظ بجرد لجميع التطبيقات والأجهزة الخاضعة لسيطرته والتي تستخدم لتخزين معلومات Citi و/أو معالجتها و/أو نقلها.

ب. يجب على المورّد التأكد من الاحتفاظ بجرد للأصول المعلوماتية الخاصة بشركة Citi تحت سيطرته وفقًا لإجراءات تُستخدم لضمان دقة واكتمال الجرد بشكل مناسب.

ج. يجب أن يكون المورّد مسؤولاً عن حماية جميع معلومات Citi التي تقع تحت سيطرته.

د. يجب على المورّد ضمان المسؤولية عن نشاط المستخدمين بطريقة تتفق مع ممارسات الصناعة.

ه. يجب تقييد وصول المستخدم إلى حسابات البريد الإلكتروني الشخصية الخارجية من الشبكة العالمية للمورّد والتي توجد عليها معلومات Citi.

8.18 تصنيف المعلومات والتعامل معها. تصنف Citi المعلومات وفقًا للتصنيف التالي: يرجى الاطلاع على الملحق للحصول على تعريفات وأمثلة لكل تصنيف مدرج أدناه.

مقيدة	**الأكثر حساسية**
معلومات تحديد الهوية الشخصية الحساسة	
معلومات تحديد الهوية الشخصية السرية	
سرية	
معلومات تحديد الهوية الشخصية الداخلية	
داخلية	
عامة	**الأقل حساسية**

أ. بناءً على تصنيف معلومات Citi، يجب على Citi أن تعمل مع المورّد على تحديد المستوى الأمني المطلوب لحماية هذه المعلومات ويجب على المورّد ضمان وجود ضوابط كافية، إلى جانب جميع المستويات المشددة أو المعدلة التي قد تطلبها Citi.

ب. يجب تخزين المعلومات السرية أو العليا على الأجهزة التي يديرها طرف ثالث وفقًا لعقد مبرم بين الطرف الثالث وشركة Citi يحتوي على أحكام تختص بالسرية بما يتوافق مع سياسات ومعايير شركة Citi.

ج. إذا سمح المورّد باستخدام أجهزة غير أجهزة الشركة لتخزين بيانات Citi (أي الأجهزة التي تديرها أطراف رابعة)، فينبغي عليه وضع سياسة تتطلب أن تخضع لموافقة إدارة معينة ووضع إرشادات معمول بها وإجراءات مراقبة حول كيفية استخدام معلومات Citi والتصرف فيها.

د. لا يجوز تخزين سوى المعلومات المصنفة من قبل Citi باعتبارها معلومات عامة على الأجهزة المملوكة لموظفي المورّد (مثل أجهزة الحاسوب المنزلي والمساعد الرقمي الشخصي وتطبيقات الإنترنت بالهواتف المحمولة وتطبيقات البريد الإلكتروني).

ه. يجب على المورّد دائمًا حماية معلومات Citi من الوصول أو التعديل أو الحذف غير المصرح به.

و. يجب نقل معلومات Citi المحفوظة على وسائط قابلة للنقل إلكترونيًا (ETM) بشكل آمن ويجب تأكيد الاستلام. يجب على المورّد التأكد من استلام الوسائط القابلة للنقل إلكترونيًا من قبل المستلم المقصود في التاريخ المتوقع للتسليم ومواصلة المتابعة مع المستلم المقصود حتى يتم تأكيد التسليم. وفي حالة عدم تلقي الإيصال في تاريخ الاستلام المتوقع، يجب على المورّد إخطار Citi.

9.18 التهيئة الآمنة.

أ. يلتزم المورّد بالحفاظ على معيار تهيئة آمن موثق لكل الأصول مع احتمالية تخزين معلومات Citi أو معالجتها أو الوصول إليها أو نقلها.

ب. يجب على المورّد تضمين إجراءات أمان المعلومات في عملياته وإجراءاته من أجل اختيار التطبيقات والمنتجات والخدمات وتطويرها وتنفيذها.

ج. يجب أن يكون لدى المورّد إجراء بناء آمن لجميع الأنظمة التي يتم فيها تخزين معلومات Citi و/أو معالجتها و/أو نقلها.

د. يجب على المورّد الاحتفاظ بصورة آمنة أو قالب آمن لكل الأنظمة.

ه. تتم إزالة كل حسابات وكلمات مرور المستخدم الافتراضية و/أو تغييرها من الأنظمة المدعومة بواسطة المورّدين وأجهزة الشبكات والتطبيقات.

و. عمليات نشر الأنظمة الجديدة أو الأنظمة المخترقة تتم تهيئتها باستخدام صورة أو قالب معتمد.

ز. أي تغيير يُجرى على التهيئة الآمنة توافق عليه الإدارة عبر عملية إدارة التغييرات.

ح. عندما تحدث تغييرات على التهيئة الآمنة، تكون هناك عملية إخطارات تشمل المتابعة والتصحيحات.

ط. يجب أن يتضمن إجراء البناء الآمن أدوات لدعم فحوصات إعدادات الأمان الآلية/معايير بناء الإعدادات في وقت نشر الإنتاج.

10.18 متطلبات التشفير. عندما يقوم طرف ثالث بإرسال وتخزين معلومات Citi المصنفة على أنها سرية أو أعلى، يجب اتباع متطلبات التشفير. ويجب أن تكون البيانات المنقولة بين Citi والجهة الخارجية التي تتعامل معها Citi مشفرة بالكامل باستخدام أدوات أو حلول معتمدة من Citi. البروتوكولات المعتمدة وأرقام الإصدارات ذات الصلة أثناء نقل البيانات هي كما يلي:

أ. عند تبادل معلومات المصادقة والتفويض: SAML v2.0, OAuth v2.0 (التفويض فقط)،

ب. لحماية قنوات الاتصال وما يرتبط بها من تبادل المفاتيح: TLS v1.2 أو TLS v1.3. يجب تصنيف مجموعات TLS Cipher على أنها "قوية"، أو "موصى بها"، أو ما يعادلها من قبل SSL Labs أو أي مؤسسة مماثلة مع تمكين السرية التامة لإعادة التوجيه (PFS) و/أو DTLS الإصدار 1.2 و / IPSEC IKE الإصدار 2.

11.18 يجب أن تكون البيانات المخزنة باستمرار في بيئة الجهة الخارجية التي تتعامل معها Citi أو عند تبادلها مشفرة بالكامل باستخدام أدوات أو حلول معتمدة من Citi. الخوارزميات المعتمدة وأطوال المفاتيح لتشفير البيانات هي كما يلي:

أ. معيار التشفير المتقدم (AES): أطوال المفاتيح المعتمدة: 128 أو 256 بت. غير مسموح باستخدام مقياس التشفير المتقدم AES بمفتاح 192 بت. الأوضاع المقيدة: يُحظر وضع الكود الإلكتروني (ECB) إلا إذا كان مقدار النص العادي أقل من أو يساوي طول الكتلة. تشفير محرك الأقراص: يوصى باستخدام مقياس التشفير المتقدم AES بمفتاح 256 بت

ب. خوارزمية ChaCha20 (التشفير الانسيابي لحالات الاستخدام المرتبطة): أطوال المفاتيح المعتمدة: 128 أو 256 بت، مع رقم خاص 96 بت وعدد كتل 32 بت أو رقم خاص 64 بت وعدد كتل 64 بت. الحد الأقصى لحجم البيانات: 16 بيتابايت.

12.18 أنظمة تشفير المفتاح العام المعتمدة، وتبادل المفاتيح، وآليات الاتفاق، وملخص الرسائل، ووظائف الاشتقاق الرئيسية، هي كما يلي:

أ. أنظمة تشفير المفتاح العام والحد الأدنى لأحجام طول المفتاح: Rivest– Shamir–Adleman (RSA), Digital Signature Algorithm (DSA): 2048. يجب عدم استخدام خوارزمية التوقيع الرقمي DSA لتأمين بيانات Citi التي تتم معالجتها أو تخزينها خارج خوارزمية التوقيع الرقمي CitiElliptic Curve Digital Signature Algorithm (ECDSA): 256.

ب. آليات تبادل المفاتيح والاتفاقية والحد الأدنى من أحجام طول المفتاح: Diffie-Hellman (DH) / Ephemeral Diffie-Helman (DHE): 2048. Elliptic- curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE): 256.

ج. وظائف ملخص الرسالة: يُحظر إنشاء مفتاح تشفير بطول أكبر من عدد البتات العشوائية في المادة المستخدمة لإنشاء التجزئة. MD-5: مقبول لتطبيقات التوقيع غير الرقمي. محظور لإنشاء التوقيع الرقمي والتحقق منه. SHA-1: مقبول لتطبيقات التوقيع غير الرقمي والتحقق من التواقيع الرقمية القديمة. محظور لإنشاء التوقيع الرقمي. مجموعة SHA-2 ومجموعة SHA-3 و POLY-1305: مقبول لجميع تطبيقات دالة التجزئة المشفرة.

د. وظائف اشتقاق المفاتيح المعتمدة على كلمة المرور والحد الأدنى من المتطلبات: PBKDF2: الحد الأدنى لعدد التكرار 10000 مع قيمة مضافة للحماية لا يقل عن 16 بايت. HKDF: يجب أن تكون هذه الوظيفة مصحوبة بقيمة مضافة للحماية، ويجب تضمين قيمة إدخال المعلومات. SCRYPT: الحد الأدنى لعدد الجولات/عامل التكلفة هو 10. يحظر استخدام NIST SP800-108 KDF لتشفير البث. Bcrypt (للتخزين المحلي لتجزئة كلمة المرور): يجب ألا يقل الحد الأدنى لعدد الجولات/عامل التكلفة عن 10.

13.18 البريد الإلكتروني الخارجي: يمكن من خلال تشفير النقل (مثل تشفير البوابة إلى البوابة عبر بروتوكول أمان طبقة النقل (TLS)، أن يتم استيفاء متطلبات التشفير لرسائل البريد الإلكتروني الفردية التي تحتوي على معلومات Citi مع تصنيف معلومات Citi الخاص بالسرية أو أعلى، حيث لا يُسمح للمورد باستخدام برامج أو أدوات تشفير الطرف إلى الطرف المعتمدة من Citi وفقًا للوائح و/أو سياسة المورّد. بروتوكولات البريد الإلكتروني الآمنة المعتمدة هي:

أ. بروتوكول التشفير على أساس التعريف (IBE) يتميز ببريد إلكتروني مشفّر ويجب استخدامه في نطاق الحلول التي تواجه عملاء Citigroup وأنظمة البريد الإلكتروني والتسليم الإلكتروني الآمنة فقط

ب. بروتوكول أمان طبقة النقل المتبادل (MTLS) يتميز بتشفير الجلسات (لا يشفّر البيانات الأساسية للبريد الإلكتروني) وهو مخصص لاستخدام البائعين والشركاء والعملاء الذين تفاوضوا مسبقًا على استخدامه

ج. بروتوكول البريد المعرف بمفاتيح المجال (DKIM) يتميز بالمصادقة وإدارة المفاتيح وهو للاستخدام مع البائعين والشركاء والعملاء.

14.18 بالنسبة لتبادل معلومات المصادقة والتفويض، فإن بروتوكول الأمان المعتمد هو SAML v2.0. يجب أن تكون جميع عمليات التنفيذ الجديدة لـ SAML من الإصدار 2.0.

15.18 الشبكات الخاصة: يمكن اعتبار الشبكات الخاصة التي يتم تنظيمها بشكل مستقل من قِبل سلطة معترف بها والتي تفي بمعايير صناعة الخدمات المالية لإجراء الأعمال بين الأطراف المتناظرة المرخص لها أو المعتمدة (مثل سويفت أو بنك مركزي) معفاةً من متطلب تشفير معلومات التعريف الشخصية السرية في الانتقال حتى توفر تلك الشبكات البنية الأساسية اللازمة لدعم النقل المشفر دعمًا تامًا.

16.18 الصوت والفاكس: يجوز إرسال معلومات Citi المصنفة باعتبارها سرية أو عليا والتي يتم إرسالها عن طريق الفاكس أو مناقشتها في مكالمات صوتية (بما في ذلك نقل الصوت عبر بروتوكول الإنترنت [VOIP]) في صورة غير مشفرة. وعند اللزوم، ينبغي على المورّد وضع إجراءات وتوجيهات مُحددة لحماية المعلومات السرية أو العليا التي يتم إرسالها من خلال تلك القنوات.

17.18 إدارة المفاتيح.

أ. يجب تطبيق خوارزميات التشفير القياسية المُستخدمة في المجال والحد الأدنى من أطوال المفاتيح لأغراض التشفير.

ب. يجب أن يكون لدى الجهة الخارجية التي تتعامل معها Citi عملية دورة حياة إدارة مفاتيح رسمية وموثقة مع وجود ضوابط لحماية المفاتيح من الاستخدام غير المصرح به أو التعرض لها.

ج. يجب أن يكون للمفاتيح غرض فريد ولا يجب استخدامها لأي غرض آخر، مثل تشفير بيانات شركة أخرى أو للاستخدام الداخلي لطرف خارجي.

د. يجب عدم عرض مفاتيح التشفير المتماثلة والخاصة في نص واضح في أي وقت ويجب تخزينها أو نقلها في شكل مشفر باستخدام مفتاح التشفير الرئيسي (KEK) فقط.

ه. يجب تقسيم مفتاح التشفير الرئيسي (KEK) إلى مكونين رئيسيين أو أكثر وأن يتم تشفيرها باستخدام XOR قبل التوزيع ولإدخال/تحميل المفتاح يدويًا.

و. يجب فصل الوصول إلى ملفات التوقيع Keystores التي تحتوي على مفاتيح خاصة أو متماثلة بشكل صحيح مع وجود عناصر تحكم تقيّد الوصول إلى الأنظمة الشخصية أو الأنظمة المصرح بها فقط.

ز. يجب تسجيل كل طلب للوصول إلى ملفات التوقيع Keystores التي تحتوي على مفاتيح خاصة أو متماثلة وتوثيقه بتفاصيل مثل من ومتى والغرض من الوصول لأغراض التدقيق.

ح. يجب عدم استخدام الشهادات الموقعة ذاتيًا وشهادات أحرف البدل Wildcard.

ط. يجب أن تحتوي المفاتيح على فترات زمنية محددة للتشفير كما هو مشار إليه في NIST.SP.800-57pt1r5: لا يلزم أن يتطابق تغيير المفتاح مع انتهاء صلاحية المفتاح المذكور. يجب تحديث المفاتيح أو تدويرها قبل انتهاء الصلاحية لاستيعاب فترات التغيير وتضارب الجداول الزمنية وتجميد النظام.

ي. يجب تشفير الشبكات اللاسلكية باستخدام خوارزميات التشفير القياسية المُستخدمة في الصناعة.

ك. يجب على المورّدين الذين يستخدمون أي شكل من أشكال آلية التشفير استخدام الأدوات والأساليب القياسية المستخدمة في المجال لإدارة المفاتيح.

18.18 مسؤولية التحكم في الوصول. لحماية جميع أنظمة المعلومات الخاضعة للسيطرة والمستخدمة لتخزين معلومات Citi السرية أو العليا من مصدر وصول غير مصرح به و/أو الوصول إليها و/أو إدارتها و/أو معالجتها و/أو نقلها، يجب على المورّد إدارة توفير الوصول المنطقي لكل الأنظمة والتطبيقات؛ وينبغي أن تكون الضوابط موثقة بالكامل وقابلة للتدقيق وأن تمنح أقل امتياز.

أ. المورّد هو المسؤول عن حقوق الوصول الخاصة بكل المستخدمين في مؤسسته.
ب. يجب على المورّد تنفيذ ضوابط الوصول التي تضمن عدم منح المستخدمين سوى تلك الامتيازات والاستحقاقات اللازمة لأداء وظائفهم.
ج. يجب على المورّد تطبيق إجراءات تضمن إزالة جميع إمكانيات الدخول الافتراضية أو تعطيلها أو حمايتها لمنع استخدامها على نحو غير مصرح به.

19.18 إدارة وصول المستخدم. يجب على المورّد أن يدير توفير الوصول المنطقي للأنظمة والتطبيقات التي تعالج معلومات Citi السرية أو العليا و/أو تخزنها و/أو تنقلها. ويشمل ذلك ما يلي:

أ. تحديد وجرد أنظمة المصادقة المعتمدة.
ب. تتطلب كل أنواع الوصول إلى بيانات Citi الحصول على موافقة من المدير أو من ينوب عنه ومالك النظام.
ج. مزيج من المزايا/الوظائف التي قد لا تتوفر إلى مستخدم فردي لأنها تمثل تضاربًا في المصالح أو انتهاكًا لقواعد المُنشئ-الفاحص.
د. عملية مراقبة للإشراف على حقوق الوصول الممنوحة/المُلغاة لكل مستخدم على النظام وإدارتها. يُعفى المورّدون منخفضو المخاطر من هذا المطلب.

20.18 تعريف المستخدم والمصادقة.. يجب أن تصدق جميع أنظمة المعلومات الخاضعة لسيطرة المورّد على هُوية المستخدمين أو الأنظمة التي تصل إلى هذه المنصات قبل بدء أي جلسة أو معاملة حيث يمكن الوصول إلى معلومات Citi. يجب أن يكون جميع المستخدمين:

أ. معرّفين أو مُحددين بشكل فريد للمنصات التكنولوجية بواسطة مُعرّف المستخدم.
ب. مصدّق عليهم في المنصة التكنولوجية باستخدام طريقة المصادقة، ويجب على المورّد التواصل مع جهة الاتصال الرئيسية للأعمال من أجل التعرف على الطرق المعتمدة الحالية.
ج. يجب أن تكون جميع استخدامات البنية التحتية المشتركة للمصادقة (مثل تسجيل الدخول الفردي وتسجيل الدخول المختصر وخدمات المصادقة الأخرى المشتركة) وفقًا لمتطلبات المصادقة؛ ويجب على المورّد الاتصال بجهة الاتصال الرئيسية للأعمال للتعرف على الطرق المعتمدة الحالية.
د. مصادقة المستخدم على الاتصالات الخارجية: (انظر 18-8-9 الوصول عن بعد).

21.18 الوصول المؤقت المميز. يجب على المورّد أن يحتفظ بقائمة جرد لجميع الحسابات المميزة والإدارية. يجب منح تسجيل الدخول المباشر إلى مُعرّف وظيفي مُميز من خلال عملية مؤقتة للوصول المُميز. يجب أن يتبع الوصول المميز إلى أنظمة المعلومات الخاضعة للرقابة عملية إدارة الوصول ذات الامتيازات المؤقتة التي تتضمن إجراءات إصدار كلمة المرور/الحساب الموثقة التي:

أ. تقتضي أن يكون مقدم الطلب إما على قائمة المستخدمين المُعتمدين مسبقًا أو لديه موافقة في وقت الاستخدام.
ب. تتطلب تبريرًا موثقًا في بطاقة التغيير/المشكلة قبل السماح بالوصول.
ج. تتضمن مراجعة مستقلة للنشاط المنجز أثناء الوصول.
د. تتضمن عملية لإلغاء/إزالة الوصول بعد انقضاء الفترة المحددة مسبقًا فيما لا يزيد عن 24 ساعة.
ه. تسمح بتمديد فترة الوصول حتى سبعة (7) أيام تقويمية، وذلك بالنسبة لاستقرار الإنتاج وما بعد التنفيذ، على سبيل المثال ما يكون بعد عملية ترقية كبرى أو حل خاص بالتركيب/الإصلاح.

22.18 الوصول المميز الدائم. لا يمكن منح حق الوصول المميز الدائم لأحد مستخدمي نظام المعلومات الخاضع للسيطرة والمستخدم لتخزين معلومات Citi و/أو معالجتها و/أو إدارتها و/أو نقلها إلا بعد استيفاء جميع الشروط التالية:

أ. توثيق مبرّر الوصول الدائم كجزء من عملية الموافقة.
ب. موافقة مدير المستخدم ومالك/مندوب المعلومات في نظام المعلومات الخاضع للسيطرة على الوصول.
ج. عندما يتم تسجيل الدخول بمعرّف مميّز، يُحظر على المسؤولين الوصول إلى البريد الإلكتروني أو تصفح الويب أو تأدية أي وظيفة باستثناء المُصرّح لهم بالاستخدام المميّز.

23.18 يجب أن تتضمن مراجعة حقوق وصول المستخدم ما يلي:

أ. يجب على المورّد تطبيق عملية موثقة لمراجعة استحقاقات المستخدم في نظم المعلومات الخاضعة للسيطرة والمستخدمة لتخزين معلومات Citi و/أو معالجتها و/أو إدارتها و/أو نقلها، والتحقق من هذه الاستحقاقات وإزالة غير الضروري منها.
ب. يجب على المورد مراجعة جميع استحقاقات المستخدم بصورة نصف سنوية على الأقل وإزالة أي وصول غير ضروري.
ج. يجب ألا يراجع المستخدمون أو يعتمدوا استحقاقاتهم أو استحقاقات الأفراد الذين أوكلوا إليهم مسؤولية المراجعة.
د. يجب مراجعة الاستحقاقات الخاصة بجميع المعرّفات الوظيفية غير الثابتة في نظم معلومات الإنتاج/استمرارية الأعمال بصورة سنوية من قبل مالك/مندوب المعرّف.
ه. يجب مراجعة قائمة المستخدمين المُعتمدين للمعرفات الوظيفية المميزة في نظم معلومات الإنتاج/استمرارية الأعمال بصورة ربع سنوية من قبل مالك (مالكي)/مندوب (مندوبي) المعرّف.
و. بعد أن يغيّر أي موظف أي وظيفة، يتبقى أمام المورّد 21 يومًا تقويميًا لمراجعة إمكانية الوصول والاستحقاق ولإزالة الوصول إلى بيانات Citi إذا لم يعد ذلك مطلوبًا للوظيفة الجديدة.

24.18 إجراءات تسجيل الدخول الآمن.

أ. يجب تأمين معرفات تسجيل الدخول المقترنة بكلمة مرور ثابتة بعد إجراء ست (6) محاولاتٍ فاشلة لتسجيل الدخول.
ب. يجب إعادة تمكين معرفات تسجيل دخول المستخدم المقفلة من خلال خدمة إعادة تعيين قياسية للصناعة أو وظيفة أخرى مرخصة. يجب عرض نص الشعار، عند دعمه لنظام التشغيل أو التطبيق، عند جميع نقاط إدخال الشبكة حيث يقوم المستخدم مبدئيًا بتسجيل الدخول فيها أو تتم مصادقته.

25.18 نظام إدارة كلمات المرور.

أ. يجب ألا تُعرض كلمات مرور المُستخدم الثابتة على الشاشة في نص واضح.
ب. يجب عدم إنشاء ترميز صعب لكلمات المرور الخاصة بالمعرف الوظيفي التفاعلي المُميز بصيغة نصية واضحة.
ج. يجب أن تضم كلمات المرور الثابتة (بخلاف أرقام التعريف الشخصية) من ثمانية (٨) رموز على الأقل، ويجب أن تحتوي على كلٍ من أحرف وأرقام، وتكون حساسة لحالة الأحرف.
د. لا يمكن استخدام أرقام التعريف الشخصية باعتبارها الطريقة الوحيدة للمصادقة للوصول إلى أنظمة المعلومات إلا إذا كانت أرقام التعريف الشخصية ضرورية لتلبية قيود الأجهزة الفعلية (مثل لوحة المفاتيح والهاتف والبطاقة الذكية).
ه. يجب تغيير جميع كلمات المرور الثابتة كل ٩٠ يومًا تقويميًا على الأقل. يُرجى ملاحظة ما يلي أيضًا:
و. يجب على جميع أنظمة المصادقة فرض رقابة لعدم نشاط تسجيل الدخول/عدم الاستخدام على ألا تتجاوز 100 يوم إذا كان ذلك مُجديًا من الناحية الفنية. قد يتم إعادة تمكين تسجيلات الدخول المعطلة من قبل المستخدم أو وظيفة أخرى مُصرح بها.
ز. يجب أن تضمن عملية المصادقة عدم استخدام كلمة المرور نفسها ضمن التغييرات الستة (6) الأخيرة على الأقل.

26.18 استخدام الأدوات المساعدة للنظام. يجب على المورّد التأكد من تقييد والتحكم في برامج الأدوات المساعدة التي يمكن أن تتجاوز النظام وعناصر التحكم في التطبيق (مثل الإقلاع/التشغيل من الأجهزة الطرفية).

27.18 انقضاء مدة الجلسة

أ. يجب أن تتم إعادة المصادقة أو تسجيل الدخول لجميع مستخدمي نظام المعلومات الخاضع للسيطرة والمستخدم لتخزين معلومات Citi و/أو معالجتها و/أو نقلها.

ب. يجب أن يُطلب من المستخدمين إعادة المصادقة بعد فترة من عدم النشاط لا تتجاوز ٣٠ دقيقة. ويتضمن النشاط أي مدخلات إلى نقطة النهاية (ماوس، لوحة مفاتيح، شاشة تعمل باللمس، وما إلى ذلك). عندما يتم الفرض بواسطة شاشة التوقف المحمية بكلمة مرور، لا يلزم فرض التطبيق/تسجيل الدخول الفردي.

28.18 التحقق من صحة بيانات الإدخال.

أ. يجب على المورّدين وضع عناصر تحكم للحماية من التهديدات الأمنية عبر الإنترنت (أي البرمجة النصية عبر المواقع أو حقن SQL وما إلى ذلك).

ب. يجب إجراء التحقق من صحة الإدخال لجميع تطبيقات الإنترانت والإنترنت.

29.18 إنهاء وصول المستخدم.

أ. بمجرد إنهاء عمل المستخدم أو استقالته، تجب إزالة وصول المستخدم أو استحقاقاته التي تسمح بوصوله إلى بيانات Citi السرية أو العليا (تسجيل دخول المستخدم إلى سطح المكتب/ Active Directory، وتسجيل الدخول الأحادي (SSO)، والبريد الإلكتروني، وكلمة المرور التي تُستخدم لمرة واحدة (OTP)، والرموز المميزة، والوصول عن بعد) وذلك بنهاية يوم العمل التالي.

ب. إذا كان للموظف حق الوصول إلى الأنظمة التي تملكها أو تديرها Citi، فيتم إخطار Citi فورًا عند تغيير الوظيفة أو إنهاء عمل الموظف.

ج. يجب أن يكون لدى المورّد عملية قائمة واجب اتباعها لاسترداد كل الأصول عندما يتم إنهاء عمل أي شخص سواء موظف أو غير موظف أو عند استقالته.

30.18 الوصول عن بعد. يجب أن يكون لدى المورّد ضوابط نافذة للوصول عن بُعد من أجل حماية الوصول إلى الشبكات التي من شأنها أن تخزّن أو تعالج أو تنقل بيانات Citi السرية أو العليا ومن بينها:

أ. يجب حماية الوصول عن بُعد لنظم المعلومات المستخدمة لتخزين معلومات Citi و/أو معالجتها و/أو إدارتها و/أو نقلها من الاستخدام غير المصرح به.

ب. جميع أجهزة الحاسوب المحمولة وجميع أجهزة سطح المكتب التي يديرها المورّد والمستخدمة لتخزين معلومات Citi و/أو معالجتها و/أو نقلها، باستخدام الوصول عن بُعد حيث يوجد تخزين/معالجة محلية للمعلومات المُصنفة في تصنيف معلومات Citi باعتبارها سرية أو عليا، يجب تشفيرها باستخدام أداة التشفير التي تلبي معايير الصناعة.

ج. يجب أن يتم إنشاء الاتصالات عن بُعد من خلال حلول معتمدة للوصول عن بُعد والتي تستخدم مصادقة متعددة العوامل.

د. يجب أن تحتوي الأجهزة التي يديرها المورّد على جدار حماية شخصي يتم تنشيطه عند توصيله مباشرةً (أي ليس من خلال جدار حماية أو بروكسي يديره المورّد) بالإنترنت.

ه. يجب توصيل الأجهزة التي يديرها المورّد بانتظام بشبكة المورّد لتلقي وتثبيت التحديثات المنتظمة للبرامج/برامج مكافحة الفيروسات كمطلب للوصول الكامل إلى الشبكة. يجوز السماح بالوصول المحدود من أجل الغرض الصريح المتمثل في تحديث الجهاز.

و. إذا كانت الأجهزة التي لا تملكها ولا تديرها الشركة تُستخدم للوصول إلى معلومات Citi السرية أو العليا، فيجب أن تستخدم حلول معتمدة لا تسمح بتنزيل محتويات على الجهاز المحلي. ينبغي تنفيذ الضوابط التالية:

1. يُحظر تنزيل بيانات Citi على الجهاز الشخصي الذي يقع خارج نطاق الحل الذي تديره الشركة.
2. يجب على المورّد التأكد من أن هذا الوصول مؤمن إما عن طريق المصادقة القائمة على الرمز أو القائمة على الشهادة باستخدام تقنيات الوصول عن بُعد القياسية (مثل VPN و Horizon وما إلى ذلك).
3. يجب تكوين حلول الوصول عن بُعد مثل Terminal Services و VMware Horizon لتعطيل مشاركة الحافظة وتعيين محرك الأقراص Drive Mapping عبر بروتوكولات Blast و PCoIP و RDP

ز. يجب أن يتم استخدام المصادقة متعددة العوامل من جانب جميع موظفي المورّد بما في ذلك، على سبيل المثال لا الحصر، الموظفين الدائمين/المؤقتين والمقاولين والمقاولين من الباطن، الذين يحتاجون إلى وصول خاص و/أو مميز و/أو إداري إلى الأنظمة و/أو مستودعات البيانات و/أو التطبيقات و/أو البنية التحتية، بما في ذلك، على سبيل المثال لا الحصر، مسؤولو النظام ومسؤولو قواعد البيانات ومسؤولو التحكم في الوصول ومسؤولو جدران الحماية ومسؤولو مواقع الويب وما إلى ذلك، الذين يرتبطون بشكل مباشر أو غير مباشر بالخدمات المقدمة إلى Citi؛ ويجب أن يتم تسجيل هذا الوصول ومراقبته بشكل مستقل من قبل المورّد من أجل الوقوف على أي نشاط مشبوه و/أو وصول غير مصرح به وفقًا لمتطلبات Citi للمورّدين كما هو مذكور أعلاه.

31.18 سياسة المكتب النظيف والشاشة الخالية. يجب على موظفي المورّد حماية معلومات Citi بجميع أشكالها، بما في ذلك المعلومات المادية المستخدمة أو المخزنة في مكان عملهم. يتعين على المورّدين إبلاغ هذا المطلب لكل موظفيهم سنويًا على الأقل من خلال التوعية بنظم المعلومات.

32.18 السلامة من الحرائق.

أ. يجب أن يمتثل المورّد للمتطلبات القانونية والتنظيمية السارية التي تحكم الأمان المادي وخلق بيئة عمل آمنة، بما في ذلك قوانين الحريق المحلية.

ب. يجب على المورّد استخدام نظام (أنظمة) للكشف عن الحرائق والإنذار بها وإخمادها. يجب فحص النظام (الأنظمة) واختباره سنويًا.

33.18 الأمان المادي.

أ. يجب تخزين معلومات Citi في مناطق آمنة تتمتع بضوابط تقصر الوصول على الأفراد المصرح لهم فقط.

ب. يجب أن يكون لدى المورّد نظام وصول مادي موثّق وقابل للتدقيق.

ج. يجب على المورّد استخدام مزيج من أنظمة الإنذار/كشف التسلل الأمنية التي تحتوي على إنذارٍ أمنيٍ يراقبه طرف ثالث، وحراس الأمن والمراقبة عبر الفيديو حسب ما هو ملائم للبيئة والخدمات المقدمة.

د. يجب أن يكون لدى المورّد سياسة موثقة للزيارات تحتوي على شرط يُلزم جميع الزوار بتقديم هُوية يمكن التحقق منها عند الوصول وتسجيل الدخول وتسجيل الخروج.

34.18 إجراءات ومسؤوليات أمان عمليات التشغيل.

أ. يجب أن يكون لدى المورد دورة حياتية موثقة لتطوير النظام الأمني (S-SDLC) مع الالتزام بالحد الأدني من المعايير لشركة Citi، إذا كان المورد يقدم خدمات تطوير البرمجيات لشركة Citi.

ب. يجب أن يكون لدى المورّد إجراءات موثقة لإدارة التغيير.

ج. يجب أن يكون لدى المورّد إجراءات موثقة لإدارة القدرات بما يتوافق مع معايير الصناعة ذات الصلة.

د. يجب على المورّد، حيثما أمكن، التأكد من أن جميع بيئات التطوير والاختبار والإنتاج منفصلة ماديًا و/أو منطقيًا عن بعضها البعض.

35.18 ضوابط الحماية من تهديدات البرامج الضارة. يجب على المورّد التأكد من اتخاذ الاحتياطات اللازمة لمنع واكتشاف إدخال أي تعليمات برمجية ضارة (مثل الفيروسات أو الفيروسات المتنقلة أو فيروسات حصان طروادة أو برامج الإعلانات المتسللة أو برامج التجسس أو برامج الفدية أو أي هجمات إلكترونية مماثلة يمكن أن تُفقد فيها البيانات)، ويجب وضع ضوابط تحكم للوقاية والاكتشاف والاسترداد للحماية من التعليمات البرمجية الضارة. يجب على المورّد:

أ. تطبيق وتحديث وصيانة تقنية لمكافحة الفيروسات ومكافحة برامج التجسس على جميع أجهزة الحاسوب الشخصية وتقنية على جميع خوادم الشبكة المحلية (LAN) وخوادم البريد وغيرها من الأجهزة التي تخزن معلومات Citi و/أو تعالجها و/أو تنقلها.

ب. وضع إعدادات أمان وتطبيقها لمنع المستخدمين النهائيين من تعطيل برامج مكافحة الفيروسات/ مكافحة البرامج الضارة وعمليات الفحص المجدولة.

ج. وضع إجراءات آلية مُدارة مركزيًا لتهيئة وتحديث برامج مكافحة الفيروسات ومكافحة البرامج الضارة

د. تنفيذ العمليات لتحديد ومعالجة أجهزة الكمبيوتر غير المتوافقة التي تكون قد انتهت عليها صلاحية توقيعات برامج مكافحة الفيروسات ومحركات الفحص.

36.18 ضوابط الحماية من التعليمات البرمجية المتنقلة. يجب على المورّدين التأكد من اتخاذ الاحتياطات اللازمة للتحكم في استخدام التعليمات البرمجية المتنقلة. عندما يُصرح باستخدام التعليمات البرمجية المتنقلة، يجب، كحدٍ أدنى، أن تلبي الإعدادات جميع معايير الصناعة والالتزامات التعاقدية تجاه Citi ويضمن أن التعليمات البرمجية المتنقلة المصرح بها تعمل وفقًا لسياسة أمنية موثقة ومحددة بوضوح ويمنع تنفيذ التعليمات البرمجية المتنقلة غير المُصرح بها.

بالنسبة للتعليمات البرمجية المتنقلة التي قد تؤثر على نظام التشغيل الأساسي أو المنصة (أي خارج "آلية تحديد الوصول SANDBOX")، يجب على المورّد التحقق من الآتي: يجب أن تكون التعليمات البرمجية المتنقلة التي ينشرها المورّد تحمل توقيع سلطة إصدار الشهادات المعتمدة لدى Citi ويجب أن تتم إدارة صلاحية الشهادة من قبل المورّد لمعالجة انتهاء سريان الشهادة أو دورانها. يجب إزالة التعليمات البرمجية المتنقلة الموقعة التي انتهى سريان شهاداتها من الإنتاج.

37.18 تسجيل التدقيق. يجب على المورّد ضمان أن تكون كل نظم المعلومات الخاضعة للسيطرة والمستخدمة للوصول إلى معلومات Citi و/أو تخزينها و/أو معالجتها و/أو إدارتها و/أو نقلها تستخدم مسارات تدقيق على مستوى البنية الأساسية أو التطبيق لتسجيل العناصر التالية:

أ. الإجراءات المتعلقة بأمان البنية التحتية للمنصة المرتبطة

ب. جميع إنذارات النظام المرتبطة بجدار الحماية أو نظام كشف التسلل/نظام منع التسلل التي أوجدت الحدث الأمني

ج. جميع محاولات انتهاك أمان النظام (مثل المحاولات الفاشلة لتسجيل دخول المستخدم)

د. جميع الأحداث المهمة المتعلقة بالمعاملات المالية ومعلومات Citi التي تتضمن على وجه التحديد العناصر التالية:

1. تحديثات المعاملات المالية
2. تحديثات بيانات معلومات التعريف الشخصية السرية
3. تحديثات البيانات المقيّدة
4. تحديثات بيانات المصادقة

ه. يجب الحصول على أدوات الإنترنت خلال فترة الاتصال (عنوان IP على الأقل أو المعلومات الأخرى ذات الصلة) مثل مُعرّف الجهاز الفريد، عندما يكون ذلك ممكنًا من الناحية الفنية، وتسجيلها من أجل تطبيقات Citi المواجهة (المواقع الإلكترونية وتطبيقات الأجهزة الجوالة) لدعم عمليات التحقيق في الاحتيال. يجب الحصول على هذه الأدوات لمعاملات Citi ولنشاط فتح الحساب الخاص بشركة Citi. يجب أن تُجمع المعلومات حتى يمكن ربط أدوات فترة الاتصال بالمعاملة أو فتح الحساب.

و. يجب تسجيل الأحداث المهمة الخاصة بإدارة أمن المعلومات تحديدًا بما في ذلك العناصر التالية:

1. إنشاء حساب المستخدم
2. تعديل حقوق الوصول الخاصة بالمستخدم
3. حذف وإنشاء وتعديل ملفات التعريف لنظام معلومات خاضعة للسيطرة.
4. إعادة تعيين كلمة المرور
5. التغييرات التي تطرأ على تكوين أمن النظام
6. يجب تسجيل جميع الأنشطة التفاعلية للمُعرّفات الوظيفية المميزة.
7. يجب أن تحتوي سجلات الأمان على المعلومات التالية على الأقل بغض النظر عن النظام الذي يُنشئ السجل ما لم يكن ذلك ممكنًا من الناحية الفنية:
   أ. تاريخ ووقت الحدث (بالتوقيت العالمي الموحد)
   ب. هُوية المستخدم للشخص الذي يقوم بالإجراء
   ج. نوع الحدث
   د. اسم الأصل أو المورد المتأثر
   ه. نوع الوصول (حذف، تعديل، وما إلى ذلك)
   و. نجاح أو فشل المؤشرات السبع لنجاح الحدث. المصدر (المحطة الطرفية، المنفذ، الموقع، عنوان IP، اسم المضيف، إلخ.)

38.18 حماية معلومات السجل. يجب على المورّد التأكد من وجود ضوابط الوصول للحفاظ على سلامة مسارات التدقيق أثناء البدء والإغلاق وأثناء التخزين والنقل.

أ. لمنع التعديلات غير المصرح بها في سجلات التدقيق، يجب على المورّد التأكد من أن السجلات لا يمكن التعديل عليها بالكتابة أو تعديلها من قبل مستخدمي النظام الذين يقومون بتتبع نشاطهم.

ب. يجب على المورّد تحديد فترة استبقاء بيانات السجل والمحافظة عليها والامتثال لها بما يتوافق مع سياسة إدارة السجلات لدى شركة Citi وجميع المتطلبات القانونية والتنظيمية السارية.

ج. يجب أن تكون ساعات جميع أنظمة معالجة المعلومات ذات الصلة داخل المؤسسة أو المجال الأمني متزامنة مع مصدر زمني دقيق.

39.18 استخدام نظام الرصد. يجب الحصول على الأحداث التالية وتسجيلها ومراجعتها بشكل مباشر أو من خلال عملية مراجعة آلية:

أ. جميع إنذارات النظام المرتبطة بجدار الحماية أو نظام كشف التسلل/نظام منع التسلل التي أوجدت الحدث الأمني

ب. جميع التحديثات للموارد المهمة كما هو محدد في البنية القياسية الآمنة.

ج. جميع الأنشطة التفاعلية التي يتم إجراؤها من خلال المُعرّفات الوظيفية المميزة أو المعرّف المؤقت.

د. استثناءات:

1. إزالة الاستحقاقات من المستخدم أو الدور أو ملف التعريف. إذا تم تنفيذ نشاط إدارة أمان المعلومات من خلال منظومة آلية لسير العمل/نظام تحقيق يحتوي على ضوابط سلامة شاملة.

40.18 ارتباط السجل والمراجعة

أ. عندما يشغّل حدث مسجل تنبيهًا، تكون قد تمت مراجعة الحدث ويكون تم تعقب تحقيقات وإجراءات المتابعة، ويشير ذلك إلى احتمالية وقوع حادث ضار بشأن أمان المعلومات.

ب. يجب أن يضمن المورّد أن سجلات التدقيق مُجمعة في نظام إدارة سجلات مركزي مثل نظام معلومات الأمن وإدارة الأحداث (SIEM) أو أداة تحليل السجلات لتحليل ارتباط السجل ومراجعته. وقد تعد ميزة لدى نظام إدارة السجلات المركزي الخاص بها أو قد تكون أداة منفصلة. يُعفى المورّدون منخفضو المخاطر من هذا المطلب.

ج. يجب على المورّدين مرتفعي المخاطر مراجعة وضبط تهيئة نظام معلومات الأمان وإدارة الأحداث (SIEM) أو أداة تحليل السجلات بصفة دورية لتحسين عملية تحديد الأحداث القابلة للتنفيذ.

41.18 التحكم في برامج التشغيل.

أ. يجب على المورّد أن يضمن عدم استخدام أي أنظمة وبرامج تشغيل سوى أنظمة وبرامج التشغيل التي يتم دعمها حاليًا من قبل مقدم خدمات تجاري مقبول في المجال أو التي لديها إصدار نشط وملائم من التصحيحات وتحديثات التكوين المتوفرة لمعالجة مشكلات الأمان.

ب. يجب على المورّد ضمان تنفيذ عملية موثقة تحدد الفترات الزمنية التي يتم خلالها تطبيق جميع تصحيحات وتكوينات الأمان المعتمدة.

ج. بغض النظر عن أي اتفاقية صيانة منفصلة بين المورّد و Citi، يجب على المورّد التأكد من أن البرامج التي تم تطويرها لـ Citi والمحكومة بموجب اتفاقية ترخيص لا تتطلب استخدام إصدارات من البرامج غير المدعومة ذات الثغرات الأمنية المعروفة وأنه يتم تحديثها وتصحيحها كما هو مطلوب في الوقت المناسب.

د. يجب الحصول على برامج التطبيقات مفتوحة المصدر المستخدمة في معالجة معلومات Citi من الموردين المعتمدين ويجب دعمها.

42.18 أمان تطوير البرمجيات..

أ. يجب أن يكون لدى مورد البرامج دورة حياة تطوير البرامج (SDLC) موثقة ومحدثة معتمدة من الإدارة.

ب. يجب مراجعة الأمان في كل مرحلة من مراحل دورة حياة تطوير البرامج (SDLC)

ج. يجب تطبيق ممارسات التشفير الآمنة.

43.18 إدارة المخاطر والثغرات الأمنية إذا كان المورّد يحتفظ بمعلومات Citi السرية أو يخزنها على موقع ويب أو نظام يمكن الوصول إليه عبر الإنترنت، فمن أجل الحماية من الثغرة الأمنية أو التهديدات التي تتضمن منتجات أو خدمات تؤثر على Citi (يُشار إليها باسم "ثغرة أمنية") يجب على المورّد الامتثال للمتطلبات التالية. على وجه العموم، يجب على المورّد:

أ. تعيين موظف مورد واحد على دراية بأمور أمان الكمبيوتر للرد على استفسارات Citi المتعلقة بأمان الكمبيوتر.

ب. بذل الجهود المعقولة تجاريًا لرصد المصادر حسنة السمعة فيما يتصل بالمعلومات حول ثغرات أمان الكمبيوتر مثل FIRST و CERT / CC والقوائم البريدية للبائعين، وذلك بصفة منتظمة، واتخاذ التدابير المناسبة للحصول على الخدمة ذات الصلة واختبارها وتطبيقها وتقديمها إلى Citi والحزم والتصحيحات والترقيات والحلول.

ج. اختبار تنفيذ تدابير أمان المعلومات، على أساس ربع سنوي على الأقل، وذلك باستخدام أدوات فحص الثغرات الأمنية في الشبكة والنظام والتطبيق و/أو اختبار الاختراق.

د. السماح لـ Citi بأن تقوم، على نفقة Citi وفي أوقات معقولة، بتقييمات للثغرات الأمنية أو الاختراقات الأخلاقية أو أي تقييمات أمان أخرى، للتحقق من امتثال المورّد لالتزاماته بموجب أي عقد وبموجب هذه المتطلبات، بما في ذلك على سبيل المثال لا الحصر، مراجعة السياسات والعمليات والإجراءات، والتقييم في الموقع لترتيبات الأمان المادي، ومسح الثغرات الأمنية في الشبكة، والنظام، والتطبيق، واختبار الاختراق، باستخدام الأدوات المتاحة تجاريًا و/أو الممارسات القياسية في المجال لإجراء عمليات الفحص هذه.

ه. الاحتفاظ، لمدة لا تقل عن 180 يومًا (أو لفترة أطول وفقًا لما يقتضيه القانون أو العقد) بملفات السجل التفصيلية المتعلقة بجميع الأنشطة على أنظمة المورّد بما في ذلك، على سبيل المثال لا الحصر:

1. جميع الجلسات التي تم إنشاؤها
2. المعلومات المتعلقة باستقبال معلومات محددة من مستخدم أو نظام آخر
3. محاولات مصادقة المستخدم الفاشلة
4. محاولات غير مصرح بها للوصول إلى الموارد (البرامج والبيانات والعمليات وما إلى ذلك)
5. إجراءات المسؤول
6. الأحداث التي تم إنشاؤها (مثل الأوامر الصادرة) لإجراء تغييرات في ملفات تعريف الأمان و/أو مستويات الأذونات و/أو تكوينات أمان التطبيق و/أو موارد النظام.

و. يجب حماية جميع ملفات السجل من الوصول أو التعديل أو الحذف غير المصرح به. بالإضافة إلى ذلك، الاحتفاظ بالسجلات المتعلقة بالخصوصية أو تقييمات مخاطر معلومات الأمان الأخرى وكذلك السجلات المتعلقة بالإجراءات والتحقيقات الأمنية الروتينية، إذا كان ذلك ممكنًا وعندما يكون ممكنًا، وفقًا لسياسة إدارة السجلات في Citi، بما في ذلك فترة الاحتفاظ المطلوبة بهذه السجلات حسبما تحددها Citi.

ز. عندما يستخدم المورّد مقاولين أو مقاولين من الباطن لتقديم الخدمات، يجب على المورّد، وعلى نفقته الخاصة، التأكد من إكمال أي تقييمات للثغرات الأمنية تكون مطلوبة بموجب هذه المتطلبات طيه، وذلك بنفس الطريقة وفي الوقت المناسب كما لو كان المورّد هو من يقدم تلك الخدمات مباشرة، ويجب أن يضمن المورّد أن اشتراط قيام أي مقاول أو مقاول من الباطن بتلك التقييمات يجب تدوينه والنص عليه في الاتفاقية المبرمة بين المورّد والمقاول/المقاول من الباطن فيما يتعلق بالخدمة، بما في ذلك الصياغات اللغوية والنصوص التي تسمح لـ Citi بإجراء مثل هذه التقييمات.

ح. في حالة الاستحواذ على المورّد ـ أو استحواذ المورّد على كيان آخر، في أي عملية اندماج أو استحواذ أو معاملة مماثلة، مع احتمالية تأثير هذه المعاملة على الخدمات، يجب على المورّد إخطار Citi كتابيًا على الفور ويجب على المورّد إجراء تقييم لأمان المعلومات على الكيان الناتج بما يتفق مع هذه المتطلبات من أجل التأكد من أن هذا التغيير لا يؤثر على الامتثال لهذه المتطلبات.

ط. **تنفيذ العمليات.** يجب على المورّد تنفيذ عملية إدارة الثغرات الأمنية والتهديدات التي تعالج و/أو تتضمن بشكل شامل كل ما يلي: (أ) اكتشاف الثغرات الأمنية وإدارتها لكل الأصول التي يمكن أن تُستخدم لمعالجة بيانات Citi السرية أو العليا أو تخزينها أو الوصول إليها أو نقلها؛ (ب) شرط إجراء عمليات مسح شهرية على الأقل باستخدام أداة تكتشف حالات حدوث الثغرات الأمنية المعروفة حاليًا؛ (ج) تصنيف الثغرات الأمنية بحسب "نظام تسجيل الثغرات الأمنية المشتركة (CVSS) الإصدار v3.0"(راجع https://www.first.org/cvss)، وفقًا لجداول زمنية تصحيحية بناءً على مدى خطورتها؛ (د) شرط اختبار إصلاح الثغرات الأمنية قبل نشر الإنتاج بالكامل؛ (هـ) عملية طارئة لتصحيح الثغرات الأمنية الحرجة؛ (و) إذا استضاف المورّد بيانات Citi السرية أو العليا على تطبيقات وبنية تحتية قائمة على استخدام الإنترنت، ينبغي إجراء تقييم سنوي حول الثغرات الأمنية (يُشار إليه باسم "اختبار الاختراق") يتم إكماله بواسطة المورّد أو طرف خارجي متخصص في هذه الأنواع من التقييمات؛ (ز) يجب أن يتتبع المورّد الأصول التي تقترب حالتها من حالة "انتهاء العمر الافتراضي" (EOL) أو حالة "انتهاء دعم البائع/المورّد" (EOVS) أو تصل إلى تلك الحالات والتي لديها عمليات قائمة لترقية هذه الأصول أو استبدالها.

ي. **الإخطار.** عندما يحدد المورّد وجود ثغرة أمنية تتعلق بمنتج أو خدمة تؤثر على Citi، يقوم المورّد بإخطار Citi كتابيًا في غضون 48 ساعة من وقوفه على تلك الثغرة، ويتضمّن إخطاره وصفًا للإجراءات العلاجية التي يتخذها المورّد. عندما يدرك المورّد وجود ثغرة أمنية تنطوي على منتج أو خدمة تؤثر على Citi عقب الإفصاح العام المسؤول عن قنوات العملية (نشر الثغرة الأمنية في قاعدة البيانات الوطنية للثغرات الأمنية (NVD) أو عبر كتالوج التهديدات المقدم إلى مزودي الحلول الأمنية الخارجيين)، يقوم المورّد بإخطار Citi كتابيًا خلال 48 ساعة من تاريخ ذلك النشر. سوف يتضمن كل إخطار معلومات حول الثغرة الأمنية، وما إذا كانت الثغرة تؤثر على Citi، وما إذا كان من الممكن استغلالها عن بُعد؛ ودرجة الثغرات والمخاطر الأمنية الشائعة (CVE). سوف يستمر المورّد في تقديم التحديثات إلى Citi حتى يتم إصلاح الثغرة الأمنية. وفي الحالات التي تحدد فيها Citi ثغرة أمنية، قد تقدم Citi إشعارًا إلى المورّد بذلك، ويجب على المورّد معالجة هذه الثغرة على الفور وفقًا لهذا القسم.

44.18 المعالجة. عندما يحدد المورّد وجود ثغرة أمنية، يقوم المورّد بإخطار Citi كتابيًا في غضون 48 ساعة من وقوفه على تلك الثغرة، ويتضمّن إخطاره وصفًا للإجراءات العلاجية التي يتخذها المورّد. بالنسبة لكل إخطار عن الثغرات الأمنية يتم تقديمه بموجب هذا القسم، سيقوم الطرف المُخطر بتقييم مستوى المخاطر وتأثير هذه الثغرة بناءً على شدتها ومخاطرها على Citi وتعيين مستوى أولوية للمخاطر بناءً على "نظام تسجيل الثغرات الأمنية المشتركة (CVSS)" على النحو المنصوص عليه في الملحق (أ) لذلك النظام، (انظر https: //www.first.org/cvss). بمجرد تعيين مستوى المخاطر والاتفاق عليه، يقوم المورّد بمعالجة أي ثغرة متوسطة أو عالية أو حرجة تم تحديدها. حيثما أمكن، يجب توفير الإصلاح لأي ثغرة أمنية مؤثرة ضمن حزمة أمان فيما يتصل بالإصدار المنشور حاليًا. إذا كان المورّد غير قادر أو غير راغب في معالجة الثغرة الأمنية على النحو الذي ترضى عنه Citi خلال الإطار الزمني المحدد، فيجوز لـ Citi إنهاء الترخيص المعمول به دون أي مسؤولية أخرى أو التزام مالي (بالنسبة للجزء الذي تم فسخه) ويجب على المورّد أن يرد إلى Citi على الفور ذلك الجزء من رسوم الترخيص المدفوعة بالنسبة والتناسب.

45.18 ضوابط شبكة أمان الاتصالات.

أ. يجب أن تكون شبكات المورّد المستخدمة للوصول إلى معلومات Citi و/أو تخزينها و/أو إدارتها و/أو معالجتها و/أو نقلها محمية من التهديدات ويجب الحفاظ على نظام الأمان لنظم المعلومات باستخدام الشبكة. وهذا يشمل المعلومات المتنقلة عبر الشبكة.

ب. يجب ألا يتم تخزين المعلومات المصنفة على أنها من معلومات Citi السرية أو العليا باستمرار على نظام يوجد بمنطقة آمنة مراقبة (DMZ) مواجهة للإنترنت.

ج. وفيما يتعلق بالشبكات المستخدمة للوصول إلى معلومات Citi و/أو تخزينها و/أو إدارتها و/أو معالجتها و/أو نقلها، يجب على مورّد معلومات Citi ضمان ما يلي:

د. إمكانية توصيل الشبكات المحلية اللاسلكية (WLAN) أو غيرها من حلول الأجهزة اللاسلكية التي تتضمن عناصر تحكم معقولة لحظر الوصول غير المصرح به (PEAP-TLS أو EAP-TTLS، وما إلى ذلك) بالشبكات التي تحتوي على معلومات Citi.

ه. أن تكون جميع وصلات IP الخارجية الموصلة إلى الشبكة العالمية للمورّدين محمية ببرنامج جدار وقائي للحماية يديره المورّد.

و. تطبيق نظام لكشف التسلل (IDS) في الوقت الحقيقي أو نظام لمنع التسلل (IPS) يراقب ويحمي اتصالات الإنترنت بالشبكة التي يتم فيها الوصول إلى معلومات Citi أو إدارتها أو تخزينها أو معالجتها أو نقلها.

ز. يجب أن تكون جميع تطبيقات وخدمات الإنترنت الموسومة بعلامة Citi التجارية المستضافة في مواقع المورّدين خدمات مكافحة لهجمات حجب الخدمة الموزع (anti-DDoS) المعتمدة لدى Citi أو عناصر تحكم مشابهة تم التحقق منها بواسطة Citi.

ح. يجب تكوين برامج جدار الحماية الخارجية باستخدام قاعدة "رفض الكل" الافتراضية. ويجب أن تكون قواعد برامج الحماية قائمةً على مبدأ الامتياز الأقل وكل محاولات الاتصال المرفوضة بواسطة جدار الحماية (مثل إفلات حزم البيانات).

46.18 الفصل داخل الشبكات.

أ. يجب على المورّد التأكد من أن جميع نظم المعلومات والتطبيقات المستخدمة للوصول إلى معلومات Citi و/أو تخزينها و/أو معالجتها و/أو إدارتها و/أو نقلها والتي يمكن الوصول إليها عبر الإنترنت لا يمكن الوصول إليها إلا عبر المنطقة الآمنة المراقبة (DMZ) الخاصة بالمورّد.

ب. خلال أحداث الطوارئ، لا بد أن يكون المورّد قادرًا على تصفية الوصول بين أجزاء الشبكة للحد من الأثر الناجم عن الأحداث الأمنية على الشبكة (مثل تصفية المنافذ أثناء تفشي الفيروسات).

ج. يتطلب الوصول عن بُعد وأمن المضيف تنفيذ ضوابط التحكم في الوصول القائمة على المجموعة (على سبيل المثال، الموظفين والمقاولين من الباطن) لتقييد الوصول إلى موارد الشبكة في شبكة المورّد. على مستوى المضيف، يمكن تطبيق التحكم في الوصول على مستوى المجموعة أو الفرد.

47.18 تحديد الأجهزة في الشبكات.

أ. يجب على منصات التكنولوجيا تحديد ومصادقة تكنولوجيا النظراء التي تتناسب مع مستويات مخاطر نظم المعلومات الخاصة بالتفاعل والضوابط الأخرى الأقل حدة.

ب. لا يجوز الوصول إلى شبكة المورّد التي يتم فيها تخزين معلومات Citi أو معالجتها أو نقلها إلا من خلال أجهزة المورّد (أي الأجهزة المادية، بما في ذلك، على سبيل المثال لا الحصر: أجهزة الحاسوب المكتبية وأجهزة الحاسوب المحمولة) التي تمتثل لهذه المتطلبات والمصرح بها من قبل المورّد.

ج. لا يجوز الوصول إلى شبكة المورّد التي يتم فيها تخزين معلومات Citi أو معالجتها أو نقلها إلا من خلال أجهزة المورّد (أي الأجهزة المادية، بما في ذلك، على سبيل المثال لا الحصر: أجهزة الحاسوب المكتبية وأجهزة الحاسوب المحمولة ووسائط تخزين البيانات القابلة للإزالة) التي تمتثل لهذه المتطلبات والمصرح بها من قبل Citi.

48.18 تحليل ومواصفات متطلبات الأمان

أ. يجب على المورّد تضمين إجراءات أمان المعلومات في عملياته وإجراءاته من أجل اختيار التطبيقات والمنتجات والخدمات وتطويرها وتنفيذها.

ب. يجب أن يكون لدى المورّد إجراء بناء آمن لجميع الأنظمة التي يتم فيها تخزين معلومات Citi و/أو معالجتها و/أو نقلها.

ج. يجب أن يتضمن إجراء البناء الآمن أدوات لدعم فحوصات إعدادات الأمان الآلية/معايير بناء الإعدادات في وقت نشر الإنتاج.

49.18 المعاملات عبر الإنترنت.

أ. عند الاقتضاء، يجب أن يكون لدى المورد نظم معلومات تستخدم كلمات مرور ديناميكية أو شهادات رقمية للتحقق من صحة بيانات الاعتماد.

ب. يجب أن تُستبدل أعمار جميع الشهادات مرة واحدة على الأقل كل سنتين (٢).

ج. بالنسبة لجميع اتصالات المواقع المواجهة للإنترنت والاتصال من نقطة إلى نقطة بين Citi والمورّد، يجب استخدام شهادات التحقق الممتد (EV).

د. *يجب على جميع تطبيقات المورّدين التي يمكنها تخزين معلومات Citi أو معالجتها أو إدارتها أو الوصول إليها أو كذلك التي يمكنها استضافة تطبيقات الإنترنت التي تحمل علامة Citi التجارية أو التي لديها اتصال بموارد شبكة Citi اتباع ما يلي:

ه. حيازة طريقة مصادقة قائمة على أنواع البيانات/الوظائف التي يتم الوصول إليها؛

و. إجراء تقييم امتثال للمصادقة متعددة العوامل (MFA)؛

ز. تطبيق حل إدارة الأنشطة المشبوهة (SAM) عبر الإنترنت

ح. في كل الحالات، ينبغي على المورّد الاتصال بجهة الاتصال الرئيسية للأعمال للتعرف على المتطلبات الحالية.

50.18 إجراءات التحكم بالتغيير.

أ. يجب على المورّد ضمان توجيه تغييرات التكوين التي تطرأ على جدران الحماية وأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) عبر عملية إدارة التغيير الخاصة بالمورّد.

ب. ويجب تسجيل الدخول الممنوح للإنتاج من خلال مُعرّفات مؤقتة ورصده من أجل تتبع التغييرات التي يتم إجراؤها في البيئة.

ج. بالنسبة لنظم المعلومات الخاضعة للرقابة التي تحتوي على معلومات العملاء المصنفة بواسطة Citi باعتبارها سرية أو عليا أو إحدى قيم مكونات مخاطر نظم المعلومات لتحقيق "السلامة"، أو ذات "إتاحة" عالية، يجب مراجعة السجلات التي يتم حفظها وفقًا للقسم ١٠-٧ ف (تسجيل التدقيق) بواسطة المورّد على أساس العينات. وقد تستند هذه المراجعات إلى منهجية مناسبة من منهجيات أخذ العينات القائمة على المخاطر.

د. ويجب أن تتحقق المراجعة من أن التغييرات التي تعتبر جزءًا من الوصول المميز المؤقت قد تم إجراؤها على النحو المنشود.

51.18 تسريب المعلومات يجب أن يكون لدى المورّد معيار ترميز آمن موثوق يمنع تسريب المعلومات، بما في ذلك:

أ. معلومات مفصلة عن النظام (مثل نوع الخادم والتكنولوجيا).

ب. عمليات تتبع التكدس وأخطاء الاستثناء التي تكشف عن بنية هيكل الدليل ونوع قاعدة البيانات الأساسية.

52.18 بيانات الاختبار. لا يجوز للمورد استخدام أو تخزين المعلومات السرية أو المعلومات ذات المخاطر العالية على النحو المحدد من قبل Citi في بيئات تطوير أو اختبار تطبيق (تطبيقات) البرامج ما لم يتم إلغاء تحديد هذه المعلومات و/أو إخفاؤها و/أو تشويشها باستخدام الأدوات والطرق التي تفي بمعايير الصناعة بما يجعل هذه البيانات لم تعد حساسة أو يجعلها تطبق نفس الضوابط كنظام إنتاج.

53.18 نقل البيانات. لا يجوز للمورد إرسال معلومات سرية أو معلومات ذات مستوى مخاطر أعلى عبر أي شبكة عامة (مثل الإنترنت) بطريقة غير مشفرة. في حالة إرسال معلومات سرية أو ذات مستوى مخاطر أعلى على النحو المحدد من قبل Citi عبر الشبكات العامة، يجب تشفير تلك المعلومات باستخدام خوارزمية تشفير وقوة واستعادة البيانات ومخازن المفاتيح التي تتوافق مع سياسات ومعايير Citi و/أو بروتوكولات التشفير القياسية في المجال المتفق عليها.

54.18 وصول موظفي المورّد إلى أنظمة معلومات المورّد. يجب أن يتم استخدام المصادقة متعددة العوامل من جانب جميع موظفي المورّد بما في ذلك، على سبيل المثال لا الحصر، الموظفين الدائمين/المؤقتين والمقاولين والمقاولين من الباطن، الذين يحتاجون إلى وصول خاص و/أو مميز و/أو إداري إلى الأنظمة و/أو مستودعات البيانات و/أو التطبيقات و/أو البنية التحتية، بما في ذلك، على سبيل المثال لا الحصر، مسؤولو النظام ومسؤولو قواعد البيانات ومسؤولو التحكم في الوصول ومسؤولو جدران الحماية ومسؤولو مواقع الويب وما إلى ذلك، الذين يرتبطون بشكل مباشر أو غير مباشر بالخدمات المقدمة إلى Citi؛ ويجب أن يتم تسجيل هذا الوصول ومراقبته بشكل مستقل من قبل المورّد من أجل الوقوف على أي نشاط مشبوه و/أو وصول غير مصرح به وفقًا لمتطلبات Citi للمورّدين كما هو مذكور أعلاه.

55.18 تخزين البيانات خارج الشبكة. يجب على المورّد، عند تخزين معلومات Citi السرية أو المعلومات ذات مستوى مخاطر أعلى خارج شبكة المورّد (مثل النسخ الاحتياطية للتعافي من الكوارث)، التأكد من أن هذه المعلومات يتم تشفيرها في حالة السكون باستخدام خوارزمية تشفير معتمدة من Citi و/أو بروتوكول تشفير قياسي مستخدم في المجال متفق عليه وقوة ومخزن مفاتيح.

56.18 متطلبات إجراءات الأعمال للوصول عن بعد لدى المورّد.

أ. إذا قدم المورّد خدمات تعهيد عمليات الأعمال وتلقى موافقة كتابية صريحة من Citi للسماح لموظفي المورّد بالاتصال عن بُعد من موقعهم (مثل العمل من المنزل) بأنظمة المورّد التي بمقدورها الوصول إلى البيانات السرية أو ذات مستوى مخاطر أعلى و/أو تخزينها و/أو نقلها (مثل بيانات الخصوصية والمعاملات النقدية وما إلى ذلك) يجب استيفاء متطلبات الأمان التالية للعناصر القابلة للتطبيق المتعلقة بالوصول عن بُعد الذي يوفره المورّد. يجب على المورّد تقديم وثائق كاملة بما في ذلك، على سبيل المثال لا الحصر، الرسوم التخطيطية لهندسة الشبكة وتدفقات البيانات وأنظمة المصادقة وأنظمة الأمان وأي تفاصيل أو تصديقات فنية أخرى قد تكون مطلوبة، وفقًا لتقدير Citi، لضمان الامتثال لمعايير Citi والحفاظ على الوضع الأمني الخاص بـ Citi.

ب. يجب أن تلبي حلول الوصول عن بعد الخاصة بالمورّد، كحد أدنى، ما يلي:

1. توفير أو إنشاء اتصال شبكة خاص ومؤمن بين الشركات إلى Citi. يجب أن يفي هذا الاتصال بمعايير الاتصال بالشبكة الخاصة بطرف ثالث وأن تتم مراجعته والموافقة عليه من قبل مكتب كبير موظفي أمان المعلومات في Citi.
2. استخدام جميع اتصالات الشبكة للتشفير الشامل باستخدام خوارزميات التشفير المعتمدة من Citi
3. ضمان أن شبكة وأنظمة المورّدين تتضمن أنظمة موحدة لإدارة التهديدات/كشف التسلل والوقاية منه، جنبًا إلى جنب مع تسجيل ورصد أنظمة الأمان هذه للتهديدات والحالات غير الطبيعية وتوثيق إجراءات الاستجابة المناسبة للحوادث واختبارها من أجل توفير الحماية والكشف والاحتواء والاستجابة والتعافي في الوقت المناسب.
4. وجود حل شبكة افتراضية خاصة VPN للوصول عن بُعد آمن ومرن (لا توجد نقطة فشل واحدة) VPN يتطلب مصادقة متعددة العوامل ("MFA") بما يتوافق مع معايير المصادقة متعددة العوامل MFA الخاصة بـ Citi. بالإضافة إلى ذلك، يجب أن يضمن حل الوصول عن بُعد هذا ألا يُستخدم للاتصال عن بُعد وأداء الخدمات ذات الصلة بـ Citi سوى (على سبيل المثال، تكوين الأمان وإدارة التصحيح والحماية من الفيروسات وإدارة تحديد الوصول وجدران الحماية وما إلى ذلك) المملوكة للمورد والخاضعة لإدارته والمعتمدة من جانبه والتس يقوم بصيانتها. في حالة استخدام رموز البرامج المميزة للمصادقة متعددة العوامل MFA، مثل تطبيق برمجي على جهاز محمول، يجب أن يصادق برنامج مصادقة الرمز الرقمي على المستخدم (على سبيل المثال، عن طريق كلمة المرور، والقياسات الحيوية، وما إلى ذلك)، ويمنع استخدامه إذا كان الهاتف المحمول مكسور الحماية أو متجذرًا (باستخدام نظام تشغيل غير تلك المعتمدة والموفرة من قبل بائع الجهاز المحمول).
5. يجب، كحد أدنى، تقديم وثائق كاملة بما في ذلك، على سبيل المثال لا الحصر، جميع الرسوم التخطيطية لشبكة الوصول عن بعد ذات الصلة، وتدفقات البيانات وجميع عناصر التحكم

والتكنولوجيات التشغيلية والأمنية، وتقديمها إلى Citi للمراجعة والموافقة عليها قبل تقديم أي خدمات وصول عن بعد لموظفي المورّد.

6. يجب على جميع موظفي المورّد الذين يستخدمون الوصول عن بُعد التصديق والموافقة من خلال أدلة موثقة على ما يلي:

أ. الامتثال لقواعد السلوك الخاصة بالطرف الثالث، وسياسة الاتصالات الإلكترونية، وجميع سياسات ومعايير Citi المعمول بها.

ب. الاحتفاظ بمساحة عمل خاصة ومخصصة عن بُعد لا تحتوي على أي أجهزة مساعدة صوتية (مثل Alexa)، و/أو أجهزة تسجيل الفيديو، و/أو أي صور أو فيديوهات أو أجهزة استماع/تسجيل صوتية أخرى. عدم السماح لأي شخص غير مصرح له بعرض أي بيانات أو أنظمة أو تطبيقات قد تظهر على شاشة (شاشات) أنظمة الحوسبة عن بُعد.

ج. إغلاق الجهاز الحاسوبي عند ترك الجهاز دون مراقبة للتأكد من تخفيف الوصول غير المصرح به لعرض الشاشة بشكل مناسب.

7. حصر الوصول عن بُعد على الأجهزة الحاسوبية (مثل الكمبيوتر المحمول) والتي يملكها ويديرها الموظفون والمورّد. وسوف تقيد هذه الأجهزة الحاسوبية المستخدم بحيث لا يمكنه استخدامها إلا في الخدمات (مثل الحل التابع جزئيًا المؤمّن) التي تكون مطلوبة صراحةً لأداء المهام المناطة به لأداء تلك الخدمات. وعلى وجه التحديد، يجب تكوين نظام الحوسبة عن بُعد لمنع المستخدم من تجاوز حل الأمان "التابع جزئيًا"، ومنع أي طباعة عن بُعد، ومنع استخدام أجهزة التخزين المحمولة الخارجية (على سبيل المثال، محركات الأقراص المصغّرة ومحركات الأقراص الثابتة المحمولة وقارئ بطاقات SD، إلخ)، ومنع أخذ لقطات الشاشة، ومنع النسخ/اللصق خارج حل سطح المكتب الافتراضي VDI الخاص بـ Citi، ومنع تثبيت أي برنامج، ومنع أي تغييرات في التكوين غير مصرح بها على النظام. يجب أن يضمن المورّد الحفاظ على نظافة الإنترنت المناسبة لأنظمة الحوسبة عن بُعد هذه من خلال التحديثات المناسبة وفي الوقت المناسب وتصحيحات الأمان وتحديثات التكوين وما إلى ذلك. كما يجب أن يطلب الجهاز الحاسوبي عن بُعد من المستخدم إعادة المصادقة بعد 30 دقيقة كحد أقصى من عدم النشاط، مع تنفيذ حماية نقطة النهاية لمنع إدخال أي تعليمات برمجية ضارة واكتشافها والتعافي منها (مثل الفيروسات أو الفيروسات المتنقلة أو فيروسات حصان طروادة أو برامج الإعلانات المتسللة أو برامج التجسس). عدم السماح باستخدام الأجهزة الحاسوبية المملوكة شخصيًا لموظفي المورّد (مثل أجهزة الكمبيوتر المحمولة/أجهزة سطح المكتب التي يُطلب من الموظفين إحضارها بأنفسهم "BYOD") لتوفير الخدمات.

8. التأكد من إجراء عمليات تسجيل ورصد كافية لتتبع نشاط المستخدم ونقطة النهاية من خلال الموقع وعنوان IP وتسجيلات الدخول/انقضاء مدة الجلسة والأنشطة المشبوهة والبرامج الضارة وما إلى ذلك. تسجيل جميع محاولات انتهاك أمان النظام (مثل المحاولات الفاشلة لتسجيل دخول المستخدم عن بعد).

ج. في حالة سماح المورّد بإدارة تكنولوجيا المعلومات عن بُعد (مثل الشبكة والنظام والتطبيق وقاعدة البيانات وما إلى ذلك)، يجب على المورّد التأكد من أن جميع عمليات الوصول عن بُعد يتم إجراؤها فقط من قبل الأفراد المعتمدين عبر اتصال مشفر وآمن (مثل الشبكة الخاصة الافتراضية VPN، وواجهة سطح المكتب الافتراضية VDI، إلخ) يتطلب مصادقة متعددة العوامل MFA، وتتم مراقبة جميع الأنشطة بحثًا عن أي نشاط مشبوه.

57.18 قبول النظام. يجب أن يطبق المورّد عمليات موثقة لإدارة نطاق المشروع وقبول النظام بما يتوافق مع معايير الصناعة ذات الصلة.

58.18 الإبلاغ عن مواطن الضعف في أمان المعلومات. يجب أن يطبق المورّد عملية تضمن **إبلاغ Citi على الفور**بأي نقاط ضعف في التطبيقات والبنية التحتية قد تؤدي إلى الإضرار بأصول معلومات شركة Citi.

59.18 المسؤوليات عن الحوادث الأمنية والإجراءات المتخذة حيالها. يجب أن يضمن المورّد تطبيق نهج فعال لإدارة حوادث أمان المعلومات التي تؤثر على معلومات Citi. يجب على المورّد توفير العمليات اللازمة التي تمكنه من الاستجابة لحوادث أمان المعلومات وإخطار Citi بها في غضون فترة زمنية متفق عليها بأي حادث أمني مشتبه في احتمالية تصنيفه بدرجة خطورة عالية وقد ينطوي على مخاطرة ملحوظة تجاه عملاء Citigroup أو حق الامتياز (بما في ذلك عندما تنطوي الحادثة على عدد كبير من العملاء؛ مبلغ كبير بالدولار؛ من المحتمل أن يكون موضوع تغطية صحفية؛ أو من المحتمل أن يؤدي إلى إخطار غير روتيني للجهة التنظيمية) في غضون ساعتين ويجب الإبلاغ عن جميع الحوادث الأمنية الأخرى في غضون ما لا يتجاوز 24 ساعة من اكتشاف تهديد أمان المعلومات أو الثغرة الأمنية في أمان المعلومات على مدار 24 ساعة 7 أيام في الأسبوع. ويشمل هذا، على سبيل المثال لا الحصر، حوادث أمان المعلومات أو تهديدات أمان المعلومات أو نقاط ضعف أمان المعلومات الناتجة عن أنظمة كشف التسلل (IDS)/أنظمة منع التسلل (IPS)/الكشف عن انحراف السلوك في الشبكة (NBAD).

60.18 الإبلاغ عن الحوادث الأمنية.

أ. يُطلب من المورّدين الإبلاغ عن أي حادث أمني يهدد أو يعرض للخطر سرية أو سلامة أو توفر البيانات السرية أو العليا التي تمتلكها أو تديرها Citi، أو البيانات التي يقع على Citi التزام أمني بشأنها، أو أنظمة المعلومات التي تحتوي على البيانات المذكورة؛ بغض النظر عن كيفية وقوع الحادث الأمني أو المتسبب فيه (موظف Citi أو بائع أو شريك Citi) أو مكان وقوعه (داخل أو خارج ممتلكات Citi). ويشمل هذا، على سبيل المثال لا الحصر، أي تغيير أو إتلاف أو إفصاح عن أو ضياع أو سرقة أو إساءة استخدام للبيانات أو الأنظمة أو الأجهزة أو الوسائط المادية أو الإلكترونية التي تحتوي على هذه البيانات. يمكن أن يشمل ذلك أيضًا الأصول التي يتعامل الجمهور معها مباشرة لأي تصنيف للبيانات، وكذلك أي معلومات تعريف شخصية (PII) / (بيانات شخصية) خرق للبيانات حيث من المحتمل أن يؤدي إلى مخاطر عالية على حقوق وحريات الأشخاص الطبيعيين، حيث تكون تلك الحقوق والحريات محددة وفقًا للقوانين أو اللوائح المحلية.

ب. يجب على موردي الطرف الثالث إبلاغ إدارتهم بأي حوادث أمنية فعلية أو محتملة، والذين يجب عليهم إخطار مسؤول Citi على الفور في حالة وجود أي إفشاء فعلي أو محتمل عن معلومات سرية أو عليا خاصة بـ Citi. يجب على ممثل Citi إخطار مسؤول أمان المعلومات على الفور.

61.18 الحماية ضد تسريب البيانات (DLP).

أ. يجب أن يطبق المورّد ضوابط تفادي تسيرب البيانات (DLP)، بما في ذلك مراقبة المحتويات والنقاط النهائية التي تغطي كل الموظفين الذين يمكنهم الوصول إلى بيانات Citi السرية أو العليا.

ب. يجب أن يكون لدى المورّد ضوابط قائمة لاكتشاف و/أو منع حالات تسرب بيانات Citi السرية أو العليا خارج شبكتها عبر القنوات التالية:

1. رسائل البريد الإلكتروني غير المشفرة.
2. مرفقات البريد الإلكتروني غير المشفرة.
3. تحميل بيانات Citi على الويب.
4. طباعة بيانات Citi.
5. نقل بيانات Citi إلى مواقع خارج شبكتها (على سبيل المثال عبر FTP).
6. محاولات نسخ بيانات Citi السرية أو العليا إلى وسائط قابلة للإزالة مثل محركات أقراص USB، ومحركات الأقراص الصلبة القابلة للإزالة، ومحركات أقراص CD/DVD، وغيرها من الأجهزة القابلة للإزالة التي بها قدرات تخزين بيانات.
7. يجب أن يشمل حل تفادي تسريب البيانات (DLP) إرسال سجل وتنبيه إلى المورّد بكل الأحداث التي تمثل محاولات (ناجحة أو محظورة) لنقل أو تحويل أو نسخ بيانات Citi السرية أو العليا من شبكتها إلى وجهات أخرى.

62.18 تصفح الويب.

أ. يجب أن يكون لدى المورّد ضوابط قائمة للوصول إلى الويب لمنع مشاركة معلومات Citi السرية أو العليا والتعرض لتهديدات البرامج الضارة أو الهجمات للموظفين الذين يمكنهم الوصول إلى بيانات Citi.

ب. أما بالنسبة للموظفين الذين يمكنهم الوصول إلى بيانات Citi السرية أو العليا:

1. يجب تسجيل كل طلبات عناوين URL.
2. يجب حظر محاولات الوصول إلى المواقع التي يمكن استخدامها لمشاركة بيانات Citi غير المصرح بها (مثل بريد الويب، والدردشة، ووسائل التواصل الاجتماعي، والتخزين عبر الإنترنت، إلخ...).
3. ينبغي حظر الوصول إلى المواقع التي من شأنها أن تعرض البيئة إلى تهديدات البرامج الضارة أو الهجمات.
4. يجب حظر محاولات الوصول إلى المواقع التي تعتبر غير مرتبطة بالعمل.
5. يجب على المورّد الاشتراك في خدمة تصنيف عناوين URL التي يتم تحديثها بانتظام؛ يتم افتراضيًا حظر كل عناوين URL غير المصنفة أو يتم حظر كل عناوين URL بشكل افتراضي ويتم التصريح بعناوين URL على أساس كل حالة على حدة. يُعفى المورّدون منخفضو المخاطر من هذا المطلب.
6. يتم دعم متصفحات الويب التي يستخدمها المورّد دعمًا كاملاً ويتم تحديثها وفقًا لآخر تحديثات الأمان بواسطة مورّد البرامج.

63.18 الرسائل الإلكترونية لا يجوز استخدام الرسائل الفورية أو شبكات نظير إلى نظير أو غيرها من أدوات الإنترنت التعاونية لنقل أو تخزين معلومات Citi خارج شبكة المورّد أو الشبكات التي تحتوي على معلومات Citi، ما لم يتم تطبيق تشفير ملائم على جميع بيانات Citi وفقًا للقسم 18-7 (سياسة استخدام عناصر التحكم في التشفير).

64.18 البريد الإلكتروني. يكون لدى المورّد ضوابط قائمة للبريد الإلكتروني لمنع مشاركة معلومات Citi والتعرض لتهديدات البرامج الضارة أو الهجمات. ويشمل ذلك ما يلي:

أ. يتم فحص مرفقات الملفات الواردة التي تدخل بوابة البريد الإلكتروني ويتم حظرها إذا كانت تشكل خطرًا على النظام.

ب. برنامج تصفية البريد الإلكتروني (مكافحة البريد الإلكتروني العشوائي، مكافحة التصيّد الاحتيالي) قيد الاستخدام ومُحدّث.

ج. يجب تشفير أي بيانات سرية أو عليا خاصة بشركة Citi عند إرسالها خارج المؤسسة.

د. يتم دعم عناوين عملاء البريد الإلكتروني التي يستخدمها المورّد دعمًا كاملاً ويتم تحديثها وفقًا لآخر تحديثات الأمان التي يوفرها بائع البرامج.

65.18 الوسائط القابلة للإزالة.

أ. يجب على المورّد حماية معلومات Citi بغض النظر عن الوسائط المحتفظ بالمعلومات عليها. ينطبق هذا المعيار، على سبيل المثال لا الحصر، على الأنواع التالية من الوسائط التي تحتوي على المعلومات: البطاقة، أو الكاسيت، أو القرص المضغوط (CD)، أو قوائم فحص المخزون، أو القرص المرن، أو غيرها من أجهزة التخزين القابلة للإزالة أو النسخ المطبوعة أو القرص المغناطيسي أو الشريط المغناطيسي أو الميكروفيلم أو الميكروفيش أو القرص الضوئي أو الوثيقة الورقية.

ب. يجب عدم منح إمكانية الوصول إلى الإعدادات الافتراضية للوصول إلى الوسائط/أجهزة التخزين المحمولة للأنظمة التي يتم فيها تخزين معلومات Citi. إذا تم منح استثناءات وبالتالي تم السماح بالوصول مع القراءة والكتابة، فيجب تشفير البيانات على جهاز الوسائط المحمولة.

ج. إذا كان مسموحًا باستخدام الوسائط القابلة للإزالة، فهذا الاستخدام يجب أن يخضع لعملية موافقة الإدارة، بما في ذلك منطق الأعمال الذي يتطلب استخدام الوسائط القابلة للإزالة.

د. يجب جرد الوسائط القابلة للإزالة.

ه. يجب تشفير الوسائط القابلة للإزالة التي تشمل بيانات Citi السرية أو العليا تلقائيًا دون إلزام المستخدم بأي إجراء.

66.18 التخلص من الوسائط.

أ. عندما تصير معلومات Citi المصنفة على أنها سرية أو عليا مؤهلة للتخلص منها وفقًا للتعليمات المقدمة من Citi (أي عندما تصبح المعلومات غير مطلوبة من Citi أو غير مفيدة لها، بالإضافة إلى أي فترة استبقاء إضافية مطلوبة بموجب القانون و/أو اللوائح و/أو سياسات Citi) يجب على المورّد إتلاف هذه المعلومات بطريقة تجعلها غير صالحة للاستعمال وغير قابلة للاسترداد.

ب. يجب استخدام أداة معتمدة تستبدل عشوائيًا قطاعات الأقراص بأحرف معينة ومختلفة لمسح الوسائط القابلة للتركيب بشكل آمن بناءً على القواعد التالية:

1. بالنسبة للوسائط التي تخزن معلومات مصنفة باعتبارها سرية أو عليا، يجب أن تستكمل الأداة ثلاث مراحل من الوسائط.
2. إزالة المغنطة من الوسائط.

ج. إتلاف الوسائط فعليًا لجعلها غير صالحة للقراءة (أي فرم الأوراق، تكسير الأقراص).

د. يجب تجميع وسائط التخزين الورقية وغير الإلكترونية الأخرى التي تشمل معلومات سرية أو عليا وتخزينها في "حاوية سرية" آمنة قبل التخلص منها نهائيًا. يجب دائمًا إغلاق الحاويات السرية بأقفال بحيث لا يمكن فتحها إلا بواسطة الموظفين المصرح لهم.

ه. يجب كذلك حذف المعلومات من أجهزة التصوير والفاكس والطابعات وأي أجهزة أخرى بها ذاكرة/سعة تخزين قد تشمل معلومات سرية أو عليا خاصة بشركة Citi.

67.18 التدابير الإضافية للتعامل مع البيانات.

أ. يجب على المورّد ضمان إخفاء كافة البيانات الحساسة من الشاشات والأوراق (ويشمل ذلك مثلاً تقارير الرصد والتجاوزات والتقارير التنظيمية وغيرها من التقارير).

ب. يجب على المورّد تقييد طباعة البيانات الحساسة أو تسجيلها أو نسخها، بما في ذلك ما يكون باستخدام "الأجهزة الخاصة" بالمورّد. يجب أن يبذل المورّد كل الجهود المعقولة لإعادة جميع معلومات Citi أو إتلافها في وقت زمني متفق عليه خلال الاتفاقية أو عند انتهائها.

68.18 إدارة أمان المعلومات والتدريب.

أ. يجب أن يضمن المورّد حصول كل الموظفين، بما في ذلك المقاولين والموظفين المؤقتين، على التعليم والتدريب التوعوي الملائم حول السياسات والإجراءات التنظيمية ذات الصلة بمهامهم الوظيفية.

ب. ويجب أن يضمن كذلك مراجعة وتحديث البرنامج التدريبي والتعليمي سنويًا.

ج. وكحد أدنى، يجب أن يتضمن المواضيع التالية:

1. الاستخدام المقبول للأصول
2. التمييز بين المعلومات والتعامل معها
3. النقل الآمن (بريد إلكتروني آمن، مخزن SharePoint آمن، عدم إرسال بيانات مملوكة لشركة Citi إلى بريد إلكتروني شخصي)
4. الإبلاغ عن الحوادث المتعلقة بأمن المعلومات
5. مكان عمل آمن (استخدام ملائم للإنترنت، برامج غير مصرح بها، عدم تنزيل برامج لا تصرح بها شركة Citi)
6. إدارة كلمات المرور (كلمات مرور قوية، مشاركة كلمات المرور)
7. ضوابط البرامج الضارة
8. الهندسة الاجتماعية (التصيّد الاحتيالي، التصيّد الاحتيالي الموجّه، والتصيّد الاحتيالي عبر الهاتف وعبر الرسائل النصية)
9. العمل عن بُعد (اتصال آمن/موثوق، أمان الجهاز الشخصي)

د. يجب أن يضمن المورّد إكمال كل الموظفين، بما في ذلك المتعهدون والموظفون المؤقتون، للتدريبات التوعوية حول أمان المعلومات في غضون 30 يومًا من تاريخ التوظيف.

ه. يجب أن يضمن المورّد إكمال كل الموظفين، بما في ذلك المتعهدون والموظفون المؤقتون، تدريبًا تنشيطيًا سنويًا.

و. يجب أن يتضمن التدريب مقياسًا لمدى فعاليته.

69.18 برنامج إدارة المخاطر السيبرانية. يجب على المورّد أيضًا، وكحد أدنى، توفير برنامج مناسب لإدارة المخاطر الإلكترونية يتضمن ما يلي:

أ. وضع برنامج لإدارة مخاطر أمان المعلومات محدد تحديدًا جيدًا وموثق و/أو برنامج لإدارة مخاطر التشغيل يحتوي على مكوّن محدد بوضوح لإدارة المخاطر السيبرانية/المعلوماتية، والذي يحدد المستوى المقبول لدى المورّد من المخاطر السيبرانية ويضمن أن المخاطر السيبرانية المتبقية تتوافق مع ذلك المستوى المقبول من المخاطر.

ب. برنامج قوي لإدارة المخاطر الأمنية يتضمن، على سبيل المثال لا الحصر، جمع و/أو أداء عمليات تدقيق ومراجعات الأمان التي تقيّم الحالة الأمنية العامة داخل المؤسسة، وتقديم تقارير بشكل روتيني سنويًا على الأقل إلى قيادتها التنفيذية للمراجعة والتأكد من عدم انتهاك المستوى المقبول من المخاطر السيبرانية لدى المورّد

ج. ضمان الامتثال لمعايير أمان بيانات صناعة بطاقات الدفع PCI-DSS المطبقة على المورّد حيث يقوم المورّد بمعالجة و/أو تخزين و/أو نقل معاملات بطاقات الائتمان/الخصم و/أو المدفوعات و/أو المعلومات.

د. وضع خطة لإدارة الأزمات ودليل لفريق الاستجابة للحوادث الأمنية (SIRT) بما يتفق مع معايير الصناعة لضمان أن يتوافر لدى المورّد القدرة الكافية والملائمة لاكتشاف حادثة أمان سيبراني واحتوائها والتحقيق فيها والاستجابة لها والتعافي منها سواء كانت هذه الحادثة مجرد محاولة أو اشتباه أو كانت حادثة فعلية وتشمل مثل تلك الحوادث الأمنية على سبيل المثال لا الحصر، برامج الفدية، والوصول غير المصرح به، واستخراج البيانات غير المصرح به، وسرقة رمز مصدر التطبيق، وما إلى ذلك.

ه. وضع برنامج فعال للنظافة السيبرانية يضمن تثبيت تصحيحات البرامج وتطبيق وصيانة تكوينات الشبكات و/أو الأنظمة و/أو التطبيقات بطريقة متسقة وآمنة.

و. وضع برنامج تعليمي وتثقيفي مناسب للأمان السيبراني (أمان الإنترنت)/المعلومات والخصوصية يتضمن، على سبيل المثال لا الحصر، منع التصيد الاحتيالي وهجمات الهندسة الاجتماعية الأخرى، والتعامل بشكل مناسب مع المعلومات السرية و/أو الخصوصية الخاضعة للنظام واللوائح، والإبلاغ عن الحوادث الأمنية وإدارة الاستجابة.

70.18 أمان التطبيقات وواجهة برمجة التطبيقات والأكواد وأمان النظام والبنية التحتية. عندما يقوم المورّد باستضافة و/أو تطوير و/أو الاشتراك في تطوير و/أو توفير بيئات التطوير و/أو تزويد تطبيقات برمجية، يجب على المورّد القيام بمراجعات التعليمات البرمجية للبرنامج المذكور و/أو تصحيحات البرنامج بحثًا عن أي عيوب أمنية، ومنع الوصول غير المصرح به و/أو أي تعديل و/أو منع إدخال البرامج الضارة أو غيرها من أشكال التعليمات البرمجية الضارة، واختبار الثغرات الأمنية للتأكد من خلو التطبيق (بما في ذلك واجهات برمجة التطبيقات)، إلى جانب خدمات النظام الأساسية ونظام التشغيل والشبكات، من الثغرات الأمنية والعيوب المعروفة التي قد يترتب عليها وقوع حادث أمني و/أو اختراق للخصوصية و/أو احتيال و/أو أي وصول غير مصرح به و/أو كشف عن معلومات سرية، وفقدان سلامة المعلومات التي تتم معالجتها أو تخزينها أو نقلها بواسطة التطبيقات، و/أو فقدان التوافر الذي قد يؤثر على الجودة للمنتجات و/أو الخدمات التي يوفرها المورّد لـ Citi.

19 المبادئ التوجيهية لمكان العمل الآمن

تسري على المورّدين الذين يمكنهم الوصول إلى معلومات Citi ومعالجتها وإدارتها وتخزينها و/أو استضافة تطبيقات الإنترنت التي تحمل علامة Citi التجارية و/أو التي لديها اتصال بموارد شبكة Citi و/أو الذين يتطلبون وصول دون مرافقة إلى مرافق Citi.

يجب على المورّدين الحفاظ على الأصول المادية وغير المادية المملوكة لشركة Citi وعملائها. ولا يجوز استخدام أصول Citi والعملاء إلا للأغراض المعتمدة وبالطرق المعتمدة (على سبيل المثال، وفقًا للتراخيص والشروط والأحكام المعمول بها)، ثم فيما يتعلق فقط بالأغراض التجارية لشركة Citi ومورّديها. وتشمل الأصول النقد والأوراق المالية والممتلكات المادية والخدمات وخطط الأعمال والمعلومات الخاصة بشركة Citi ومعلومات المورّدين ومعلومات الموزعين والملكية الفكرية (برامج الحاسوب والنماذج والعناصر الأخرى) وجميع المعلومات الشخصية ومسجلة الملكية والمعلومات السرية الأخرى. يُعتبر اختلاس أصول شركة Citi أو الإفصاح غير المصرح به عنها انتهاكًا لواجبك تجاهها وقد يشكل نوعًا من أعمال الاحتيال ضد شركة Citi. وبالمثل، فإن الإهمال أو الهدر أو الاستخدام غير المصرح به لأصول Citi يمثل أيضًا انتهاكًا لواجبك تجاهها.

العنصر	المتطلبات
معلومات Citi (الوثائق الإلكترونية والورقية)	قفل معلومات Citi وتأمينها بعد ساعات العمل العادية وفي أي وقت يكون فيه المورّد بعيداً عن مكان العمل المخصص.
أجهزة الحاسوب الشخصية المكتبية (PC) وأجهزة الحاسوب المحمولة (اللابتوب)	يجب تأمين أجهزة الحاسوب الشخصية المكتبية وأجهزة الحاسوب المحمولة المستخدمة للوصول إلى أي من معلومات Citi بكلمات مرور للشاشة المؤقتة بعد فترة من عدم نشاطها. ومتى غادر المورّد مكان العمل المخصص، يجب عليه قفل الحاسوب الشخصي و/أو الحاسوب المحمول من خلال الضغط على CTRL + ALT + DEL ثم اختيار Lock Computer "تأمين الكمبيوتر". إذا كان المورّد يستخدم حاسوب محمول لعرض معلومات Citi، فيجب عليه التأكد من أنه مؤمن باستخدام كابل أو أقفال التأمين في الوحدة الأساسية خلال ساعات العمل وأنه مقفل بشكل آمن بعد ساعات العمل العادية.
قفل الخزائن	يجب قفل الخزائن والأدراج التي تخزن فيها معلومات Citi بعد انقضاء ساعات العمل العادية.
المناطق المفتوحة في المكاتب	يجب عدم استخدام المناطق المفتوحة في المكاتب كخادم ملفات/مراكز بيانات مصغرة لتخزين معلومات Citi ما لم يتم تصميمها خصيصًا لهذا الغرض وتوثيقها لدى Citi.
الطابعات وآلات النسخ الفوتوغرافي وأجهزة الفاكس	يجب إزالة جميع المواد ذات الصلة بشركة Citi من على الطابعات وآلات النسخ وأجهزة الفاكس.
التخلص من المعلومات	يلزم التخلص من معلومات Citi التي لم تعد ثمة حاجة إليها (يتعين اتباع جداول زمنية مُحددة للاحتفاظ). يجب فرم المستندات أو وضعها في سلة مهملات مؤمنة/مغلقة .ويجب التخلص من الوسائط المغناطيسية بشكل آمن بعد اتباع إجراءات المسح المناسبة.

20 الذكاء الاصطناعي/التعلم الآلي

يسري على المورّدين الذين يستخدمون الذكاء الاصطناعي/التعلم الآلي (AI / ML)، على النحو المحدد من قبل Citi في هذه المتطلبات الخاصة بالمورّدين، في أي جزء من المنتج/الخدمة التي يقدمونها.

1.20 يجب على المورّد إرسال إطار كتابي إلى Citi يحدد بوضوح الذكاء الاصطناعي/التعلم الآلي، على النحو المحدد من قبل Citi في الملحق بهذه الوثيقة، حيث يمكن لذلك الذكاء الاصطناعي/التعلم الآلي أن:

أ. يُستخدم أو يُتضمن أو يُدمج بطريقة أخرى في أي منتجات أو خدمات بموجب عقد لتقديمها بشكل مباشر أو غير مباشر إلى Citi، أو في أي جزء منها، بما في ذلك أي منتجات أو خدمات لأطراف ثالثة متضمنة أو مضمنة فيها؛

ب. يُستخدم بأي طريقة في أداء المورّد لأي عقد، بغض النظر عن استخدام الذكاء الاصطناعي/التعلم الآلي أو احتوائه أو تضمينه بطريقة أخرى في المنتج أو الخدمة الفعلية التي يتم تقديمها إلى Citi من عدمه؛

ج. يُستخدم بأي طريقة قد تعرّض معلومات Citi إلى ذلك الذكاء الاصطناعي/التعلم الآلي، بما في ذلك، على سبيل المثال لا الحصر، أي ذكاء اصطناعي/ تعلم آلي يستخدمه المورّد في عمليات أعماله غير التجارية (مثل حفظ سجلات الأعمال وتحسين العمليات والبحث والتطوير والامتثال والتدقيق الداخلي).

2.20 يضمن المورّد أن أي اتفاقية تحكم علاقته مع أي مقاول من الباطن (أو أن اتفاق ذلك المقاول من الباطن مع أي طرف آخر ذي صلة) يتم استخدامه لأداء التزامات المورّد أو المساعدة في ذلك، بموجب أي عقد أو أي اتفاق بين المورّد وطرف ثالث يحكم تقديم ذلك الطرف الثالث للخدمات لدعم أي عملية أعمال غير تجارية مُشار إليها أعلاه، تحتوي على أحكام تكون، على الأقل، بنفس القدر من الشمولية والصرامة لتلك الأحكام الواردة في هذا القسم 20، ويمارس المورّد حقوقه بموجب هذه الأحكام لصالح Citi بناء على طلب Citi. بالإضافة إلى ذلك، وطوال مدة العقد، يجب إخطار Citi بأي استخدام للذكاء الاصطناعي/التعلم الآلي كما هو موضح في القسم 20 في أي مرحلة على الفور، ويجب على المورّد الامتثال على الفور لأي طلب من Citi للحصول على مزيد من المعلومات الثبوتية المتعلقة بالذكاء الاصطناعي/ التعلم الآلي واستخدامه، وقد يخضع استخدام الذكاء الاصطناعي/ التعلم الآلي لمراجعة وتغييرات ورقابة إضافية على ذلك الذكاء الاصطناعي/ التعلم الآلي، عند الاقتضاء.

3.20 في حالة طلب جهة تنظيمية لذلك، باعتبارها جزء من أي تفتيش تنظيمي أو تحقيق جنائي في استخدام الذكاء الاصطناعي/التعلم الآلي في أي جزء من المنتج/الخدمة، يجب على المورّد مساعدة Citi في الاستجابة لطلب تلك الجهة التنظيمية، بما في ذلك إجراء و/أو تسهيل إجراء عمليات تدقيق الخوارزميات اللازمة لاكتشاف العمليات الفعلية للخوارزميات التي تكوّن نماذج الذكاء الاصطناعي/التعلم الآلي.

4.20 يجب أيضًا الالتزام بالمبادئ التالية:

أ. الشرعية. يُتوقع أن يتم تصميم أنظمة الذكاء الاصطناعي/ التعلم الآلي الخاصة بالمورّد بحيث تلتزم بالقانون المعمول به وتمتثل له، وكذلك المعاهدات الدولية الأكثر حماية لعملاء Citi ومستخدميها وموظفيها.

ب. الغرض والتناسب. سوف يتم تصميم أنظمة الذكاء الاصطناعي/التعلم الآلي الخاصة بنا لتحقيق الأغراض المقصودة من الخدمات المقدمة إلى Citi، وسوف تعمل تلك الأنظمة فقط بشكل متناسب بالقدر الضروري والملائم والمرتبط بالأغراض المذكورة أعلاه.

الملحق - التعريفات

انقطاع الاتصال: هو إجراء أمني يتم من خلاله فصل جهاز الكمبيوتر أو النظام أو الشبكة فعليًا عن أجهزة الكمبيوتر أو الأنظمة أو الشبكات الأخرى. تحد بنية النسخ الاحتياطي لبيانات الأجهزة منقطعة الاتصال من التعرض للهجمات الإلكترونية وتسمح باستعادة البيانات إلى ما كانت عليه قبل بدء الهجوم.

يشمل **القانون المعمول به**: (أ) القوانين واللوائح الحكومية بشأن حبس الرهن العقاري (ب) والقواعد والإرشادات والإصدارات الأخرى الصادرة عن مختلف الوكالات الفيدرالية بالولايات المتحدة، بما في ذلك مكتب المراقب المالي للعملة (يشار إليها أحيانًا باسم الإرشادات والمبادئ التوجيهية بشأن العلامات المنذرة) التي تنفذ القسم 114 من قانون المعاملات الائتمانية العادلة والدقيقة لعام 2003

منطقة الإتاحة هي المكان الذي يمتلك فيه مزود الخدمة السحابية مجموعة من مراكز البيانات المنطقية. منطقة الإتاحة عبارة عن مركز أو أكثر من مراكز البيانات المنفصلة التي تتمتع بطاقة إضافية وشبكات واتصالات في منطقة السحابة.

الذكاء الاصطناعي (AI) يشير إلى طريقة كمية أو نظام أو نهج كمي ("تقنيات") يحاكي الذكاء البشري عبر برامج الكمبيوتر لعمل تقديرات أو تنبؤات أو توصيات أو قرارات بأسلوب يتجاوز الأساليب الإحصائية أو الرياضية أو الاقتصادية أو المالية التقليدية. **تشمل فئات الذكاء الاصطناعي ما يلي:**

- **الذكاء الاصطناعي الآلي:** هو تقنيات "الذكاء الاصطناعي الديناميكي" التي يمكنها بالإضافة إلى ذلك تغيير هيكلها الأساسي تلقائيًا (مثل المعلّمات الفائقة ومتغيرات الإدخال)
- **الذكاء الاصطناعي المعرفي:** هو التقنيات التي يمكنها صنع القرارات بشكل مستقل واتخاذ الإجراءات وفقًا لذلك، حتى في الأمور التي لم يتم تدريبها عليها بشكل خاص
- **الذكاء الاصطناعي الديناميكي:** هو التقنيات التي يمكنها تلقائيًا إعادة تدريب المعلمات بشكل دوري في الإنتاج، وذلك على عكس "الذكاء الاصطناعي الثابت".
- **الذكاء الاصطناعي الثابت:** هو تقنيات الذكاء الاصطناعي التي يتم تدريبها يدويًا دون الاتصال بالإنترنت أو التي تتم برمجة معلماتها بشكل صريح ثم استخدامها بعد ذلك لإجراء تقديرات أو تنبؤات أو وضع توصيات أو صنع قرارات.

التعلم الآلي هو مجموعة فرعية من الذكاء الاصطناعي تستمد التمثيلات أو الاستدلالات من البيانات دون برمجة صريحة لكل تمثيل للمعلمة أو خطوة حاسوبية، مثل الغابات العشوائية والأساليب القائمة على الشبكة العصبية. في المقابل، تشتمل تقنيات الذكاء الاصطناعي التي ليست ضمن مجموعة التعلم الآلي الفرعية على تقنيات مثل المنطق الضبابي وتقنيات تحليل علاقات التبعية المعقدة لمعالجة اللغة الطبيعية.

مسؤول النشاط التجاري (BAO): أحد موظفي شركة Citi المسؤولين عن تنفيذ أنشطة معينة مقترنة بعلاقات المورّد وإدارتها بنشاط.

هدية العمل: أي عنصر له قيمه (بخلاف الأنشطة الترفيهية المرتبطة بالأعمال) يتم منحه أو استلامه بواسطة أي من موظفي Citi فيما يتعلق بأعمالها أو أعمال أي طرف خارجي باستثناء، عمومًا، العناصر التي تبلغ قيمتها 25 دولارًا أمريكيًا أو أقل.

معلومات Citi: هي المعلومات التي تمتلكهاCiti أو تلتزم بحمايتها أثناء مرحلة التخزين أو النقل أو التخلص منها سواء بالتنسيقات الرقمية أو غير الرقمية. **تصنيفاتمعلومات Citi تشمل:**

- **المعلومات السرية** هي المعلومات التي تلتزم الشركات التابعة لشركة Citi بحمايتها، بما في ذلك، على سبيل المثال لا الحصر، المعلومات التي تخص العملاء أو العاملين أو الأطراف الثالثة أو الشركات التابعة لشركة Citi.
والمعلومات السرية هي أي مجموعة من البيانات تخضع لقيود تنظيمية أو تعاقدية فيما يتعلق بالإفصاح. وهي أيضًا المعلومات التي تُقرر الشركات أنها من المُحتمل، في حال الإفصاح عنها إلى الأشخاص غير المصرح لهم، أن تؤدي إلى وجود ميزة تنافسية أو تحمل أثراً سلبياً كبيراً على العمل.
- **معلومات التعريف الشخصية السرية (CPII)** سيكون لها تصنيف لحماية المعلومات السرية إذا كان يُتوقع بشكل معقول أن يؤثر عدم تحقيق سرية معلومات التعريف الشخصية أو سلامتها أو إتاحتها سلبًا بشكل خطير على الأفراد المتضررين أو على شركة Citi، فإن عدم تحقيق سرية معلومات التعريف الشخصية أو سلامتها أو إتاحتها من شأنه أن يؤدي إلى خرق متطلبات الإخطار بموجب القانون المعمول به.

يُقصد بالتأثير السلبي الخطير على الفرد أن هذا التأثير قد يؤدي بشكل معقول إلى خسارة مالية أو عملية احتيال معتدلة، أو حرج أو ضيق شخصي. أمثلة على عناصر البيانات التي تشكل عند دمجها بمعلومات أخرى معلومات تعريف شخصية سرية:

- اسم الفرد أو معلومات الاتصال (العنوان، أو رقم الهاتف، أو عنوان البريد الإلكتروني) بالإضافة إلى:
- رقم جواز السفر، أو رقم رخصة القيادة، أو رقم إثبات هوية وطنية أو حكومية، أو رقم معرّف الضريبة للفرد؛
- رقم إثبات هوية العميل، أو رقم بطاقة الائتمان/الخصم، أو معرّفات الحساب التي قد تؤدي إلى حركات الأموال، أو رقم حساب مالي آخر؛
- عناصر بيانات المعاملات التي يمكن استخدامها لسرقة هوية أو الاحتيال بشأنها؛
- رقم طلب حساب العميل، بيانات تقرير الائتمان، درجة الائتمان؛
- معلومات تقييم أو تعويض أداء العامل؛
- تسجيلات الفيديو، وتشمل تسجيلات الدوائر التلفزيونية المغلقة CCTV وسجلات ماكينات الصراف الآلي (ATM)
- تُعتبر هذه العناصر معلومات تعريف شخصية سرية سواءً كانت بمفردها أو مع عناصر أخرى: رقم الضمان الاجتماعي الأمريكي، أو رقم إثبات هُوية صادرة عن الحكومة (والذي يعادل في استخدامه و/أو حالة الحماية القانونية رقم الضمان الاجتماعي الأمريكي) بمفرده.

- المعلومات **الداخلية** هي المعلومات التي تتم مشاركتها بصورة عامة داخل Citi، والتي لا يُقصد توزيعها لأي شخص خارج Citi، والتي تكون غير مصنّفة على أنها مقيدة أو سرية. وتتضمن أمثلة المعلومات الداخلية السياسات والمعايير التي نطبقها.
- **معلومات التعريف الشخصية (PII):** المعلومات الشخصية هي أي معلومات:
  - تحدد هوية الفرد أو الأسرة أو يمكن استخدامها لتحديد هوية أيًا منهما (مثل الاسم أو التوقيع أو العنوان أو المُعرّف الوطني الفريد مثل رقم الضمان الاجتماعي أو رقم تسجيل الإقامة أو تاريخ الميلاد أو رقم رخصة القيادة).
  - تتعلق بالفرد أو الأسرة أو تصف أيًا منهما أو يمكن اقترانها بأيٍ منهما أو يمكن ربطها بشكل معقول بأيٍ منهما (سواء بطريقة مباشرة أو غير مباشرة)؛
  - يمكن استخدامها للمصادقة على الفرد أو تقديم إمكانية الوصول إلى أي حساب (مثل اسم المستخدم أو عنوان البريد الإلكتروني أو كلمة المرور أو رقم التعريف الشخصي (PIN) أو رقم التعريف أو إجابات على أسئلة الأمان)؛ أو تتعلق بالفرد والتي قد تكون حساسة (مثل المعلومات الطبية أو الخاصة بالصحة، رقم الحساب، قيمة الحساب).

  - وتتضمن المعلومات الشخصية أيضًا المعلومات الصحية المحمية (وفقًا لتعريفها بموجب قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة في الولايات المتحدة)، والمعلومات الشخصية الحساسة ومعلومات الائتمان (وفقًا لما تحدده قوانين حماية/خصوصية البيانات والسرية المصرفية).

- **المعلومات العامة** هي المعلومات المتاحة خارج Citi دون قيود أو التي يُقصد منها استخدامها استخداماً عاماً، مثل البيانات الصحفية أو المقالات الخاصة بشركة Citi والتي يتم عرضها في الأخبار التي تخص Citi.
- **المعلومات المقيدة** هي المعلومات التي، إذا تم الإفصاح عنها لأفراد غير مصرح لهم بما في ذلك العاملين لدى Citi، قد يكون لها أثرٌ كبيرٌ على الالتزامات القانونية والتنظيمية لشركة Citi أو على مركزها المالي أو عملائها أو امتيازاتها.
- سيكون **لمعلومات التعريف الشخصية المقيدة** تصنيف لحماية المعلومات المقيّدة إذا كان يُتوقع بشكل معقول أن يؤثر عدم تحقيق سرية معلومات التعريف الشخصية أو سلامتها أو إتاحتها سلبًا بشكل خطير أو كارثي على الأفراد المتضررين أو شركة Citi أو في حالة، بموجب قانون الاختصاص القضائي، ضرورة زيادة الضوابط الأمنية نتيجة طبيعة معلومات التعريف الشخصية (مثل معلومات التعريف الشخصية الحساسة أو ذات "التصنيف الخاص"). تشمل الأمثلة على معلومات التعريف الشخصية المقيدة أي معلومات تم الحصول عليها من معلومات التعريف الشخصية العامة، ومعلومات التعريف الشخصية الداخلية ومعلومات التعريف الشخصية السرية مصحوبة بما يلي:

- البيانات المتعلقة خصيصًا بكلٍ من: الجنس، الدين، المعتقدات الدينية أو الفلسفية، العرق، الانتماءات أو الآراء السياسية، عضوية الاتحادات، معلومات عن الخلفية الجنائية أو الجرائم الجنائية، البيانات الجينية، البيانات البيولوجية، أو البيانات المتعلقة بالميول أو الأنشطة الجنسية الخاصة بالفرد.
- معلومات الحالة الصحية (PHI) التي تتضمن معلومات بشأن السجل الطبي أو الحالة العقلية أو البدنية للفرد؛ وتوفير الرعاية الصحية للفرد ودفع مقابل لتوفير الرعاية الصحية للفرد.

العميل يعني أي عميل أو زبون لشركة Citi وقد يشمل الأفراد (أي الأشخاص الطبيعيين) وكذلك الشركات والمؤسسات والمنظمات والكيانات القانونية.

منطقة السحابة هي موقع مادي يقوم فيه مزود الخدمة السحابية بتجميع مركز (مراكز) البيانات.

مُعدات وأنظمة وخدمات الاتصالات: هي أي أجهزة أو برامج أو تطبيقات تُستخدم في نقل الاتصالات الإلكترونية المكتوبة أو الصوتية أو المرئية. تشمل قنوات الاتصالات الإلكترونية على سبيل المثال لا الحصر: أجهزة الكمبيوتر أو أجهزة الكمبيوتر المحمولة أو الأجهزة اللوحية أو الأجهزة المحمولة أو الهواتف المحمولة، بما في ذلك الأجهزة الشخصية الخاصة بالموظفين التي يُطلب منهم إحضارها بأنفسهم (BYOD) وأجهزة BlackBerry والهاتف والفاكس (خدمات الفاكس) والوصول إلى الإنترانت والإنترنت وخدمات Wi-Fi وخدمات البريد الإلكتروني وخدمات والرسائل الفورية مثل رسائل Microsoft Lync و Skype و Bloomberg ومواقع الويب والتطبيقات ذات ميزات الاتصالات المضمنة أو اجتماعات الفيديو أو منصات التعاون مثل Zoom أو Microsoft Teams وخدمات الوسائط الاجتماعية وخدمات مشاركة المعلومات التفاعلية وغرف الدردشة التي توفرها أطراف ثالثة/خارجية ولوحات الإعلانات الإلكترونية والمدونات.

يُقصد **بالمحتوى** المعلومات السرية الخاصة بـ Citi وأي بيانات أو تقارير أو إحصائيات أو معلومات أخرى من أي نوع (أ) يتم تقديمها أو إتاحتها بشكل مباشر أو غير مباشر للمورد من قبل Citi أو الشركات التابعة لها أو نيابةً عنها أو نيابةً عنهم أو عن عملائهم أو زبائنهم أو مقدمي الخدمة لديهم، (ب) أو تم إنشاؤه أو إنتاجه عبر الخدمات، (ج) أو مشتق من أي مما سبق.

العقد وثيقة قانونية مكتوبة وموقعة بين طرفين أو أكثر وتشتمل على عرض وقبول ومقابل مالي والتزامات من جانب الأطراف ومشروعية الغرض. ويمكن أن تشمل نماذج العقود الاتفاقيات الرئيسية بشأن المنتجات والخدمات أو بيانات العمل/أوامر العمل أو التعديلات والإضافات أو الجداول الزمنية أو الأوامر أو أي وثيقة كتابية أخرى موقعة بواسطة كيان تابع لشركة Citi وأحد المورّدين. كما تعتبر اتفاقية عدم الإفصاح (NDA) عقدًا لأغراض هذه المعايير

اختبار حجب الوصول (DOA) يتحقق من مستوى التوظيف والدعم لعمليات أعمال Citi التي يمكن استردادها ضمن هدف وقت الاسترداد المحدد.

اختبار حجب الوصول (DOA) وهو أن تقوم شركة Citi بتسجيل دخولها إلى تطبيق للمورّد أو يقوم المورّد بإدارته أو على أنظمة المورّد، يجب على المورّد أن يجري اختبار حجب الخدمة (DOS)، مرة واحدة على الأقل سنويًا وفقًا لمتطلبات شركة Citi لكل مركز بيانات/ غرفة تقنيات ترتكز فيها هذه التطبيقات، وذلك بهدف إثبات أن التطبيق يمكن استرداده إلى موقع التعافي من الكوارث DR المُحدد في خطة التعافي من الكوارث الخاصة بالمورّد.

الاتصالات الإلكترونية هي الرسائل أو المعلومات التي يتم إرسالها أو استقبالها أو استخدامها بواسطة الموظفين باستخدام وسائل إلكترونية ويتم نقلها عبر الأسلاك أو عبر الإشارات اللاسلكية. وتشمل الاتصالات الإلكترونية على سبيل المثال لا الحصر الرسائل النصية والبريد الإلكتروني ورسائل النظير إلى نظير أو الرسائل الفورية، ومنشورات المدونات ومنشورات وسائل التواصل الاجتماعي، والرسائل التي يتم إرسالها عبر تطبيقات المراسلات مثل WhatsApp وWeChat وLine وSignal وViber، وتشمل المرفقات ولقطات الشاشة وملفات الصوت أو الفيديو المسجلة والملفات التي تم إنشاؤها أو استلامها أو تنزيلها أو تخزينها أو نقلها أو مسحها أو استخدامها عبر معدات وأنظمة وخدمات الاتصالات الإلكترونية.

المُعرّفات الوظيفية: عبارة عن معرّف عام، مثل المسؤول (ADMIN) أو الجذر (ROOT)، يستخدمه شخص أو عملية للوصول إلى نظام الأمان. تضمن عملية المبادرة الرئيسية في إدارة لهويات وإمكانية الوصول (IAM) أن يكون لدى شركة Citi ضوابط معينة ومُحددة معمول بها للحماية من المخاطر التي تحيط باستخدام المعرّفات الوظيفية.

عمليات الامتياز الحرجة/تطبيقات الامتياز الحرجة (FCA): هي تلك العمليات/التطبيقات التي تعرفّها Citi بأنها ضرورية للتنفيذ الناجح لوظائف الأعمال الحرجة المتعلقة بالامتياز.

الاحتيال: هو تصرف متعمد، سواء بتقديم معلومات خاطئة أو إغفالها بهدف خداع الآخرين، مما ينتج عنه تعرض الضحية لخسارة، أو تحقيق الجاني لمكسب.

تشمل الخدمات المستضافة أي تطبيقات مثبتة، وأي منشآت وبيئة يديرها المورّد أو يستخدمها لتوفير الخدمات المستضافة، وجميع التطبيقات والبرامج الأخرى، وقواعد البيانات، والمواقع الإلكترونية، والخوادم، والأجهزة، والشبكات، والاتصالات السلكية واللاسلكية وغيرها من المعدات، وغيرها من التقنيات المثبتة أو المستخدمة في بيئة الخدمات المستضافة، وفي كل حالة، جميع التحديثات وخدمات الدعم، باستثناء كل المحتوى وكل أنظمة Citi.

أمان المعلومات أو (IS): يُقصد به الحالة التي يكون فيها الحاسوب أو نظام الحاسوب محميًا من الهجوم أو الوصول غير المصرح به، وبسبب تلك الحالة، (أ) يظل الحاسوب أو نظام الحاسوب متاحًا وقابلًا للتشغيل؛ (ب) ويظل الحاسوب أو نظام الحاسوب محتفظًا بسلامته؛ (ج) ويتم الحفاظ على سلامة وسرية المعلومات التي يتم تخزينها أو معالجاتها أو نقلها من خلال الحاسوب أو نظام الحاسوب.

تهديد أمان المعلومات: هو تصرف أو نشاط (سواء معروف أو مشتبه به) يُجرى على الحاسوب أو نظام الحاسوب أو من خلالهما، قد يعرض أمان المعلومات الموجودة على هذا الحاسوب أو هذا النظام أو غيرهما للخطر أو يؤثر عليها سلبًا.

ضعف أمن المعلومات: هو أي ضعف يحدث في الحاسوب أو نظام الحاسوب بحيث يمكن استغلالها بواسطة تهديد واحد أو أكثر لأمن المعلومات.

يُعرّف المصطلح **غير المدرة للدخل/لغير العملاء** بأنه الأنشطة التجارية المهمة التي لا ترتبط بالأنشطة المدرة للدخل بما في ذلك الأنشطة القانونية والإشرافية والتنظيمية والمتعلقة باستمرارية الأعمال.

اتفاقية عدم الإفصاح (NDA) هي اتفاقية يتم إبرامها بين Citi والمورّد بحيث يخضع تبادل المعلومات واستخدامها والإفصاح عنها للشروط الواردة في تلك الاتفاقية.

جرد السجلات هو عبارة عن قائمة مفصلة تتضمن أنواع السجلات والموقع والتواريخ وما إلى ذلك من سجلات Citi، وتعد لازمة لأي شركة لإدارة سجلاتها بشكل صحيح من خلال دورة حياة المعلومات.

الاحتفاظ بالسجلات هو متطلب يتم فرضه على السجلات والمعلومات يُوقف إدخال أي تعديل عليها أو التخلص منها حتى يتم رفعه بواسطة السلطة التي أصدرت أمر الاحتفاظ.

قدرة الاسترداد هي حجم منتجات وخدمات المورّد أو كميتها أو سرعة تقديمها معبرًا عنه كنسبة مئوية للتسليم العادي للمنتجات والخدمات.

مدة الاسترداد هي المدة القصوى، معبرًا عنها بالأيام التقويمية، التي يكون المورّد خلالها قادرًا على ضمان استمرارية العمليات أثناء وضع الاسترداد.

هدف نقطة الاسترداد هو نقطة زمنية في الماضي، محددة بالساعات، يجب استرداد البيانات بعد انقطاع الأعمال وصولاً إليها. وهي الفترة القصوى المستهدفة التي قد تُفقد عندها البيانات من إحدى خدمات تكنولوجيا المعلومات بسبب حادث كبير. وهدف نقطة الاسترداد ما هو إلا مقياس للفترة الزمنية القصوى التي قد يتم فقدان البيانات عندها إذا وقع حادث كبير يؤثر على إحدى خدمات تكنولوجيا المعلومات. وهو لا يعد مقياساً مباشراً لكمية البيانات التي قد تُفقد، على سبيل المثال، حتى نهاية المعالجة في اليوم السابق.

هدف وقت الاسترداد هو المدة بالساعات بين وقت توقف الخدمة واستعادة المنتجات والخدمات

منظمة إدارة الموارد (RMO) تتولى مسؤولية إدارة الموارد الشاملة العالمية لشركة Citi، بما في ذلك تحديد المصادر الاستراتيجية، وعمليات الشراء حتى السداد، ومكتب التوظيف، وإطار عمل إدارة المورّدين.

مدير تعهيد منظمة إدارة الموارد (RMO) هو موظف في منظمة إدارة الموارد (RMO) يتحمل المسؤولية عن التفاوض بشأن الشروط التجارية للعقد والمتطلبات والتسعير، بما في ذلك طلبات تقديم العروض وغيرها من أنشطة اختيار المورّدين وإدارة شروط وأحكام العقد ومتطلبات اعتماد التقييم المالي.

يُقصد **بالتأثير السلبي الخطير أو الكارثي** على الفرد بأن هذا التأثير قد يؤدي بشكل معقول إلى تأثيرات سلبية ضخمة على الفرد، وتشمل الخسارة المالية أو فقد الوظيفة أو الصعوبة في الحصول على وظيفة، أو انتهاك حقوق الإنسان، أو الإهانة الشخصية أو العامة أو السجن غير المشروع.

القدرة الزمنية للتعافي التكنولوجي (TRTC) عبارة عن إجمالي وقت الاستعادة التقديري لخدمة التطبيق/الأعمال وعناصر البنية التحتية التابعة لها وذلك لتعافيها في أوقات الكوارث أو الموقع البديل بعد الاستدعاء.