

متطلبات CITI للموردين

المالك:

رئيس المشتريات والمخاطر في Citi

تاريخ الإصدار:

يناير 2015

تاريخ المراجعة:

سبتمبر 2026

الإصدار:

9

جدول المحتويات

1	لمحة عامة	3
2	تكافؤ فرص العمل	4
3	مكافحة الرشوة والفساد (AB&C)	5
4	الهدايا والترفيه	5
5	التفاعل مع الموردين ومبادئ الموردين	6
6	حظر الرق الحديث	6
7	موظفو المورد	8
8	إدارة الاحتيال	8
9	التفاعل مع وسائل الإعلام والظهور العام	10
10	الاتصالات الإلكترونية المكتوبة	10
11	الأنشطة والمساهمات السياسية	10
12	مكافحة غسل الأموال ("AML")	11
13	إدارة السجلات	12
14	مرونة المؤسسة/استمرارية الأعمال	13
15	المعايير العالمية لفحص الخلفية الأمنية	17
16	النفقات	19
17	أمان المعلومات (IS)	20
18	المبادئ التوجيهية لمكان العمل الآمن	46
19	الذكاء الاصطناعي/تعلم الآلة (بما في ذلك الذكاء الاصطناعي التوليدي/الذكاء الاصطناعي الوكيل)	47
20	شكاوى العملاء	48
21	سياسة التداول الشخصي والاستثمار	49
22	معايير الفوترة والفواتير	49
23	سياسة الغياب الإلزامي	50
	ملحق - التعريفات	51

1-1 المتطلبات العامة

توضح متطلبات Citi للموردين (يُشار إليها باسم "المتطلبات") التي بين أيدينا بعض الالتزامات التي يجب على الموردين الوفاء بها أثناء ممارسة الأعمال التجارية مع Citi. تسري بعض المتطلبات على جميع الموردين، بينما يعتمد تطبيق المتطلبات الأخرى على مورّد 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 تتم الإشارة إلى ذلك المعنى طيه، وفي هذه الحالة يكون لتلك المصطلحات المعنى المحدد لها في العقد، على النحو المعرف 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 كل منها باسم "العقد")، بالإضافة إلى أي التزامات محددة في أي اتفاقية، أو أي التزامات بموجب القانون المعمول به (حسب تعريف هذا المصطلح أدناه)، أو أي إشعار يُقدم للمورد من Citi لإبلاغ المورّد بالتزاماته بموجب ما سلفت الإشارة إليه (يُشار إلى كل منها باسم "الإشعار")، أو أي متطلبات إضافية تكون أكثر تحديدًا تنفذها وحدات الأعمال أو الوظائف في Citi. وفي حالة وجود أي تعارض بين أي من المتطلبات المذكورة أعلاه وهذه المتطلبات، تسري الالتزامات والمتطلبات الأكثر تقييدًا. يجب على الموردين 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.

يتعين على المورد الامتثال فورًا لأي طلب معقول قد يقدمه Citi إلى المورد للحصول على البيانات التي يطلبها Citi فيما يتعلق بخدمات المورد أو موظفيه تزامنًا مع التزام Citi بالامتثال للقانون المعمول به. يعتبر فشل المورد في الامتثال لهذه الالتزامات خرقًا جوهريًا لشروط هذه الاتفاقية.

قد يؤدي عدم الامتثال لهذه المتطلبات، أو أي متطلبات إضافية تحددها إحدى وحدات الأعمال التابعة لدى Citi التي يتعامل معها المورد، إلى إنهاء عقد المورد مع Citi. علاوة على ذلك، يمكن أن تُعتبر انتهاكات المتطلبات أيضًا أنها انتهاكات للقانون المعمول به وقد تؤدي إلى الوقوع تحت طائلة التعويضات عن الأضرار المدنية التي تُستحق إلى Citi (أو أطراف ثالثة) أو عقوبات جنائية على المورد. لا يجوز للمورد استخدام الامتثال لسياساته الخاصة كبديل لالتزامه بالامتثال لأي من أحكام هذه المتطلبات دون موافقة كتابية من Citi.

2-1 المتطلبات المطبقة على بعض الموردين الانتقائيين

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

رقم القسم	عنوان القسم	قابلية التطبيق
2	تكافؤ فرص العمل/العمل الإيجابي	ينطبق على العقود وأوامر الشراء اللازمة لتنفيذ عقد مبرم بين Citi والحكومة الفيدرالية الأمريكية؛ وإذا كان هناك شك بشأن ما إذا كان العقد أو أمر الشراء يشكل عقدًا من الباطن أو أمر شراء تابعًا للحكومة الفيدرالية، يتم إدراج عبارة "حسب الاقتضاء" في بداية البند أو نهايته، وفقًا لما يكون مناسبًا.
12	مكافحة غسل الأموال	ينطبق هذا على الموردين الذين يؤدون خدمات معينة تتعلق بالعملاء (مثل إجراءات التسجيل، وفحص حسابات العملاء والمعاملات) أو تسليم البيانات/المقاييس المتعلقة بالأنشطة السابقة؛ و/أو الموردين 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	ينطبق على الموردين الذين يقومون بالوصول إلى معلومات Citi ومعالجتها وتخزينها

رقم القسم	عنوان القسم	قابلية التطبيق
14	استمرارية الأعمال	تنطبق على الموردين الذين يقدمون الخدمات أو يستضيفون البنية التحتية/التطبيقات التكنولوجية التي يستخدمها Citi. يتحمل مسؤول نشاط الأعمال (BAO) في Citi مسؤولية توضيح قابلية التطبيق ومتطلبات استمرارية الأعمال (COB) للمورد.
15	المعايير العالمية لفحص الخلفية الأمنية	ينطبق هذا على الموردين الذين يقدمون خدمات إلى Citi.
16	النفقات	ينطبق هذا على الموردين المؤهلين حسب العقود الموقعة معهم للمطالبة باسترداد نفقات العمل القابلة للاسترداد.
17	أمان المعلومات (IS)	ينطبق هذا على الموردين بما في ذلك المقاولين من الباطن الذين يمكنهم الوصول إلى معلومات Citi/معالجتها/تخزينها؛ و/أو الموردين المسؤولين بصفتهم مضيفين لتطبيقات الإنترنت التي تحمل علامة Citi التجارية؛ و/أو الموردين الذين لديهم اتصال بموارد شبكة Citi؛ و/أو الموردين الذين يحتاجون إلى وصول دون مرافقة إلى مرافق Citi.
18	المبادئ التوجيهية لمكان العمل الآمن	
19	الذكاء الاصطناعي/تعلم الآلة (بما في ذلك الذكاء الاصطناعي التوليدي/الذكاء الاصطناعي الوكيل)	ينطبق هذا على الموردين الذين يستخدمون الذكاء الاصطناعي/تعلم الآلة (AI/ML)، على النحو المحدد من قبل Citi، في أي جزء من المنتج/الخدمة التي يقدمونها.
20	سياسة التداول الشخصي والاستثمار	تنطبق على الموردين الذين يحتاجون إلى الوصول المنتظم إلى MNPI كجزء من مسؤولياتهم الوظيفية في Citi.
23	سياسة الغياب الإلزامي	تنطبق هذه السياسة على غير الموظفين ("العاملون") الذين يشغلون مناصب حساسة (على النحو المعرف في المسرد "العاملون") الذين يشغلون وظائف حساسة ("، بالإضافة إلى المديرين المباشرين والمشرفين على الموظفين الذين يشغلون وظائف حساسة") المديرين ("، وجهات اتصال وحدات أعمال Citi لغير الموظفين الذين يشغلون وظائف حساسة.

2 تكافؤ فرص العمل

2-1 تكافؤ فرص العمل.

وضع Citi سياسات مصممة لضمان تكافؤ فرص العمل لجميع الأشخاص المؤهلين دون النظر إلى العرق أو اللون أو الدين أو الجنس أو التوجه الجنسي أو الهوية الجنسية أو الأصل القومي أو الجنسية أو وضع الهجرة أو العمر أو الحالة الاجتماعية أو المعلومات الجينية أو الإعاقة أو حالة المحاربين القدامى المكفولة أو أي سمة أخرى محمية بموجب القانون.

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

يقوم الموردون بمراجعة بيان سياسة تكافؤ فرص العمل في Citi بالولايات المتحدة، واتخاذ الإجراءات المناسبة بما يتوافق معه، ويمكن العثور على هذا البيان على الرابط www.citigroup.com/global/eo-aa-policy.

2-2 العقود الحكومية

يجب أن تتضمن العقود وأوامر الشراء اللازمة لتنفيذ عقد من عقود Citi مع الحكومة الفيدرالية البند التالي حرفيًا بالخط العريض كما هو موضح أدناه. (إذا لم تكن متأكدًا من كون الأمر يتعلق بعقد من الباطن/أمر شراء للحكومة الفيدرالية، أضف، من قبيل المبالغة في الحذر، عبارة "حسب الاقتضاء" في بداية القسم).

[حسب الاقتضاء]، يلتزم المورد بجميع قوانين مكافحة التمييز الفيدرالية المعمول بها ويؤكد أنه لا يدير أي برامج على نحو ينتهك أي قوانين فيدرالية معمول بها فيما يتصل بمكافحة التمييز

3-2 ملحق العقود الحكومية

يجب أن تتضمن العقود وأوامر الشراء اللازمة لتنفيذ عقد من عقود Citi مع الحكومة الفيدرالية الإشعار التالي في ملحق العقد من الباطن أو أمر الشراء. (إذا لم تكن متأكدًا من كون الأمر يتعلق بعقد من الباطن/أمر شراء للحكومة الفيدرالية، أضف، من قبيل المبالغة في الحذر، عبارة "حسب الاقتضاء" في نهاية الإشعار أدناه.) وبصفة Citigroup متعاقدًا مع الحكومة الفيدرالية، يقدم Citigroup بموجب هذا إلى المقاول أو البائع الموقع أدناه إشعارًا كتابيًا بالتزاماتنا بشأن تكافؤ فرص العمل نيابةً عن المحاربين القدامى المحميين والأفراد ذوي الإعاقة. يلتزم Citigroup بشكل كامل بالقسم 503 من قانون إعادة التأهيل وقانون مساعدة إعادة تكييف المحاربين القدامى في حقبة فيتنام، بالإضافة إلى اللوائح المعمول بها بموجب 41 C.F.R. § 60-300 و 41 C.F.R. § 60-741، على التوالي. يمكن العثور على بيان سياسة تكافؤ فرص العمل في الولايات المتحدة الخاص بنا على الرابط www.citigroup.com/global/eo-aa-policy. يمكن توجيه أي أسئلة حول التزاماتنا ببيان سياسة تكافؤ فرص العمل في Citi إلى جهة الاتصال المذكورة في بيان السياسة الخاص بنا.

[حسب الاقتضاء]، نطلب منك اتخاذ الإجراء المناسب بما يتفق مع بيان السياسة المعمول به لدينا واللوائح.

3 مكافحة الرشوة والفساد (AB&C)

يطبق Citi سياسات وإجراءات وضوابط داخلية مصممة بشكل معقول للامتثال لقوانين مكافحة الرشوة والفساد (AB&C) المعمول بها ويحظر تمامًا الرشوة أو مدفوعات التسهيل بأي شكل من الأشكال. يجب على المورد (بما في ذلك مقدمي الأعمال)، أو العاملين لديهم، أو أي شخص يعمل نيابةً عن Citi، سواء بشكل مباشر أو غير مباشر، إنجاز أنشطتهم وفقًا لأعلى المعايير الأخلاقية، وبما يتوافق مع القانون الأمريكي للممارسات الأجنبية الفاسدة ("FCPA")، والقانون البريطاني للرشوة (UKBA)، كل حسب التعديلات التي يتم إدخالها عليها، وجميع قوانين مكافحة الرشوة والفساد (AB&C) المحلية السارية في البلدان التي يعمل فيها Citi.

يحظر على المورد، وكذلك أي من موظفيه، في طور العمل نيابةً عن Citi، أو فيما يتصل بأي اتفاقية أو علاقة بين المورد و Citi القيام بما يلي: (1) دفع أو منح أو تفويض أو عرض أي مدفوعات أو مزايا أو فوائد أو أي شيء ذي قيمة آخر لأي شخص؛ أو (2) تلقي أو قبول أي مدفوعات أو مزايا أو فوائد أو أي شيء ذي قيمة من أي شخص آخر في أي من الحالة (1)-(2) على نحو يمثل انتهاكًا إلى FCPA أو UKBA أو أي قوانين أخرى لمكافحة الرشوة والفساد (AB&C). يجب على المورد وموظفيه إجراء أنشطتهم ومعاملاتهم نيابةً عن Citi، أو فيما يتعلق بأي من اتفاقيات المورد أو علاقته مع Citi، بما يتوافق مع المتطلبات، بما في ذلك هذا القسم. كما يجب على المورد وموظفيه أيضًا وضع برنامج امتثال إلى AB&C، والسياسات والإجراءات المصممة والمطبقة لضمان امتثاله لجميع قوانين AB&C.

للاطلاع على نظرة عامة حول برنامج AB&C لدى Citi، يُرجى زيارة Citigroup's Investor Relations (في قسم سياسات Citi، ثم اضغط على برنامج AB&C).

4 الهدايا والترفيه

لا يجوز للموردين، ولا لموظفيهم، تقديم الهدايا أو منح أي شيء ذي قيمة (بما في ذلك وسائل الترفيه) إلى موظفي Citi، إذ كان من شأن هذا أن يؤدي إلى تضارب في المصالح بشكل فعلي أو ظاهري أو المعاملة بالمثل أو التأثير على نزاهة الموظف أو حكمه، أو التأثير على اتخاذ القرار من جانب الموظف بشكل غير سليم بأي طريقة أخرى، أو جعل الموظف يتصرف بما يتعارض مع واجباته أو إبداء تصرفات تنتهك القوانين المعمول بها بأي وجه آخر. دون الحد من عمومية ما سبق، يجب على

الموظف الالتزام بقسم الهدايا المحظورة والترفيه ضمن G&E Standard. ويجب على الموردین وموظفهم عدم تقديم هدايا تتصل بالعمل غير نقدية تتجاوز في مجموعها 300 دولارًا أمريكيًا لكل شخص في السنة التقويمية، إلى أي موظف من موظفي Citi.

وفي حال قيام المورد بأنشطة ترفيهية مرتبطة بالأعمال (مثل دعوة لتناول وجبة طعام أو فعالية رياضية أو ثقافية أو أي من الفعاليات الأخرى المماثلة) لأي من موظفي Citi، يجب على المورد حضور هذه الفعالية كما يجب أن تكون الأنشطة الترفيهية مناسبة ومعقولة ومقبولة عرفًا وغير مبالغ فيها أو متكررة بشكل مفرط. علاوة على ذلك، إذا لم يكن المورد حاضراً في الفعالية، فسيتم اعتبار الترفيه بمثابة هدية عمل، وسوف يخضع لحدود الإبلاغ المعمول بها ضمن Citi Gifts and Entertainment Standard. لا يجوز للمورد، نيابةً عن Citi أو بزعم التصرف نيابةً عنه، تقديم أي شيء ذي قيمة، بما في ذلك ما يكون على حساب المورد نفسه أو على حساب موظف Citi، لأي شخص، سواء بشكل مباشر أو غير مباشر، أو حت أي شخص آخر على أن يحذو نفس الفعل، إذا كان من شأن عمل ذلك أن يمثل، أو من شأنه أن يُنظر إليه بشكل معقول على أنه يمثل، أمراً فاسداً أو غير مشروع أو انتهاكاً للقانون المعمول به.

5 التفاعل مع الموردین ومبادئ الموردین

<https://www.citigroup.com/citi/suppliers> يشارك Citi مع الموردین في عدد من المبادرات ويهدف لزيادة الوعي ببرنامج المشتريات لدى Citi مع الموردین المحتملين من المجتمعات التي نعمل على خدمتها. علاوة على ذلك، تسعى هذه التفاعلات إلى تحديد الموردین الواعدين، وعلى وجه الخصوص أولئك الذين يقدمون حلولاً مبتكرة لمعالجة قضايا الأعمال الناشئة. وتتوفر معلومات إضافية حول توقعات Citi بشأن الموردین على موقع [Doing Business with Citi](#) على:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 حظر الرق الحديث

يلتزم Citi بتطبيق ممارسات تهدف إلى تحديد، وتسعى إلى منع، مخاطر حدوث أشكال الرق الحديث والاتجار بالبشر داخل مؤسسته أو في سلاسل التوريد التابعة له. يلتزم موردو Citi بالمتطلبات الموضحة أدناه، وبتطوير سياسات و/أو إجراءات و/أو ممارسات فعالة على مستوى المؤسسة لتحديد، والسعي إلى منع، مخاطر الرق الحديث والاتجار بالبشر ضمن عملياتهم وسلاسل التوريد الخاصة بهم. يجب على الموردین إكمال استبيان مسؤولية الشركات لدى Citi بناءً على طلب Citi، ويشمل أي معلومات إضافية حسب الحاجة، لتمكين Citi من تقييم التعرض للمخاطر والخطوات المحتملة لتخفيف تلك المخاطر، خاصة للموردین في القطاعات والمناطق الجغرافية ذات المخاطر العالية. ومن المتوقع أن يتبع المقاولون من الباطن التابعين للمورد نفس الإجراءات.

6-1 تجنب عمالة الأطفال

لا يجوز للموردین توظيف العمالة من الأطفال. يشير مصطلح "الطفل" إلى أي شخص يقل عمره عن الحد الأدنى لسن العمل بموجب القوانين المعمول بها، أو في حالة عدم وجود تلك القوانين، أي شخص يقل عمره عن 15 عاماً أو دون سن استكمال التعليم الإلزامي، أو أيهما أكبر. 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.

6-2 حرية اختيار العمل

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

1- العقود والأجور وساعات العمل: يجب أن تُحدد شروط توظيف العمال أو تعاقدهم في وثيقة مكتوبة يسهل على العمال فهمها، وتُبين 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.

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

3- 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 ألا يتعرض العمال المهاجرون وأسرهم والأشخاص المرتبطون بهم بشكل وثيق للتمييز في شروط وأحكام عملهم على خلفية جنسيتهم.

4- الأجور والمزايا وساعات العمل: يُحدد أجر الموظف وفقاً لجميع قوانين الأجور المعمول بها، وتشمل تلك القوانين المتعلقة بالحد الأدنى للأجور وساعات العمل الإضافية والمزايا المقررة قانوناً. يجب دفع رواتب الموظفين بالكامل وفي الوقت المحدد مع تقديم كشوف رواتب شفافة. ولا يجوز خصم أي مبالغ من الأجور أو المزايا، أو استقطاعها، كإجراء تأديبي. وينبغي ألا تتجاوز أسابيع العمل الحد الأقصى الذي ينص عليه القانون المحلي، ويجب أن يكون العمل الإضافي طوعياً، وفي حدود قانونية، ويجب ألا يعاقب أي عامل على رفض العمل الإضافي.

5- عدم مصادرة وثائق إثبات الهوية: لا يجوز مصادرة أو احتجاز بطاقة هوية العمال أو تصاريح السفر أو جوازات السفر الخاصة بهم 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 لخلق أوضاع تشبه الرق في مكان العمل.

6- عدم فرض رسوم توظيف أو استبعاد المدين: لا يتحمل العمال، سواء 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 مطالباتهم بتسديد الديون عن طريق العمل. وإذا تبين أن رسوماً أو تكاليف قد تم تحصيلها من العمال فيما يتعلق بعملية التوظيف أو تكبدوها خلال فترة العمل، فعلى المورد اتخاذ التدابير المعقولة لرد تلك التكاليف على الفور. عندما تقتضي الضرورة الاستعانة بالعمال الذين يتم توظيفهم من خلال طرف ثالث، كوكالة توظيف مثلاً، فيجب ألا يُكلف بذلك إلا وكالات التوظيف حسنة السمعة. وفي الحالات التي يتم فيها الاستعانة بالعمال مباشرة، يجب أيضاً عدم تكليف سوى وكالات الاستقدام حسنة السمعة. وينطبق حظر دفع العمال لأي رسوم فيما يتصل بالتوظيف على جميع وكالات التوظيف والوكلاء الأصليين والوكلاء الفرعيين. ويجب على الموردين وضع ضوابط لضمان الامتثال. **حرية الحركة:** للعمال الحق في الحركة دون قيود غير معقولة ويجب ألا يتم حصرهم جسدياً 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.

7- 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.

1-7 تدريب موظفي المورد وتكليفهم وإعادة تكليفهم وإدارتهم

يلتزم المورد باستخدام أعداداً 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 المورد 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 الموظفين للعمل في المشاريع بطريقة تقلل إلى أدنى حد من الاضطرابات الناجمة عن الحاجة إلى إعادة توجيههم. يضمن المورد 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 يقدمها 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 المورد وحده المسؤولية الكاملة عن جميع الالتزامات المتعلقة بصفته صاحب العمل فيما يتعلق بموظفيه، بما في ذلك، على سبيل المثال لا الحصر، توفير جميع التغطيات التأمينية المطلوبة، وتقديم جميع الإقرارات الضريبية السارية، وسداد جميع المدفوعات الضريبية وإيداع الضرائب المطلوبة بطريقة تتوافق مع وضع المورد كمقاوم مستقل.

2-7 استبدال موظفي المورد

يقوم المورد باستبعاد واستبدال أي موظف يعينه المورد لمشروع ما إذا أخطر Citi المورد بأن ذلك الموظف غير مقبول من جانب Citi لأي سبب غير تمييزي. يوافق المورد 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) فوراً عندما يكون ذلك الموظف غير قادر أو غير راغب في تقديم الخدمات في الوقت المناسب وبطريقة مهنية.

3-7 سياسات شؤون موظفي المورد

يقر المورد ويضمن ويتعهد بأنه يضع ويدير بشكل فعال سياسات وإجراءات شاملة لتأهيل موظفيه الذين هم أشخاص طبيعيين 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، يقر المورد كذلك ويضمن ويتعهد بأن لديه ضوابط وإجراءات لضمان امتثال المورد الكامل لجميع القوانين المعمول بها المتعلقة بالهجرة، بما في ذلك التحقق من أن جميع موظفي المورد المكلفين بأعمال Citi مصرح لهم بالعمل طوال المهمة على نحو يتسم بالامتثال الكامل لجميع القوانين المعمول بها المتعلقة بالهجرة. بناءً على طلب Citi، يقدم المورد إلى Citi على الفور دليلاً كتابياً على تصريح العمل لأي موظف أو لجميع موظفي المورد المكلفين بأعمال Citi وامتثالهم للقانون المعمول به فيما يتصل بالهجرة، ويقوم المورد بتغيير أي موظف ليس لديه تصريح عمل متوافق مع القانون المعمول به ببديل مناسب يحل محل ذلك الموظف، بما في ذلك تقديم كل ما يلزم من تدريب وتوجيه لضمان توفير الخدمات في الوقت المناسب وبشكل فعال، وذلك في كل حالة دون أي تكلفة إضافية على Citi.

4-7 ملكية المورد

في سبيل الامتثال للقوانين واللوائح المعمول بها في الولايات القضائية التي يمارس فيها Citi أعماله، وبناءً على طلب Citi، يتعين على المورد تقديم تفاصيل المالكين، ممن هم أشخاص طبيعيين و/أو كيانات، بما في ذلك المالك (المالكين) المباشرين للمورد وصولاً إلى المالك المستفيد النهائي الذي يملك أو يتحكم في التعاقدات أو المنتجات أو الخدمات، سواء بشكل مباشر أو غير مباشر، من خلال النفوذ أو غير ذلك من الوسائل.

8 إدارة الاحتيا

فيما يتعلق بجهود Citi لتحديد مخاطر الاحتيا والتخفيف من حدتها (يُشار إليها باسم "مكافحة الاحتيا").

1-8 يجب على جميع الموردين:

- 1- التعاون مع أي تحقيقات يجريها Citi بشأن أي سرقة مشتبه بها أو مزعومة أو احتيا أو أي نشاط إجرامي أو أي مخالفة محتملة أخرى، وأي محاكمة بشأن أي سلوك احتيالي أو إجرامي إلى أقصى حد يسمح به القانون.

- 2- ضمان الإبلاغ عن أي حوادث احتيال محتملة إلى Citi في الوقت المناسب، من خلال الخط الساخن الخاص بالأخلاقيات [Ethics Hotline](#). ويشمل هذا، على سبيل المثال لا الحصر، محاولة السرقة أو الاحتيال (مثل إرسال بيانات خاطئة أو غير دقيقة أو مُحَرَّفة بشأن المورد، أو مخططات الاحتيال في الفوترة، أو اختفاء الأموال أو الأوراق المالية، إلخ) أو النشاط الإجرامي أو المخالفة الإجرامية أو الاشتباه في حدوث أي مما سبق أو ادعائه أو وقوعه فعلاً مما يتضمن Citi أو أحد موظفيه أو مورديه أو وكلائه أو التابعين له من غير موظفيه (كالموظفين المؤقتين أو المقاولين).
- 3- السماح بإجراء المراقبة والإشراف من جانب Citi وممثليه، ودعم التحقيقات التي تُجرى بمعرفة Citi - وجهات إنفاذ القانون - في نشاط الاحتيال المحتمل والذي يتورط فيه ذلك المورد.
- 4- الإبلاغ، في الوقت المناسب، عن أي تضارب في المصالح (بما في ذلك تضارب المصالح بين المورد/موظفي المورد و/أو موظفي Citi) التي يتم إعلام المورد بها؛
- 5- دعم 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 المورد الذين يقدمون خدمات تكون بطبيعتها أكثر عرضة لمخاطر الاحتيال القيام بما يلي:
 - 1- توثيق واتباع برنامج إدارة مخاطر الاحتيال الذي يحدد مخاطر الاحتيال الجوهرية ذات الصلة بالخدمات التي يقدمونها إلى Citi وكذلك الضوابط والإجراءات المعمول بها للتخفيف من هذه المخاطر.
 - 2- إكمال التدريب على التوعية بمخاطر الاحتيال (خلال 90 يوماً من تاريخ التعيين، ثم سنوياً بعد ذلك)، وتدريب الموظفين على عناصر محددة من مخاطر الاحتيال المتعلقة بالخدمات المقدمة إلى Citi.
 - 3- رصد حالات محاولات الاحتيال والالتزام بالضوابط الفعالة للتخفيف من مخاطر الاحتيال فيما يتعلق بالخدمات المقدمة إلى Citi، وتوثيق إجراءات الضوابط واختبار مدى فعالية الضوابط على أساس مستمر، مع الإبلاغ عن أي أوجه قصور إلى مسؤول نشاط الأعمال (BAO).
 - 4- تقديم أي معلومات مطلوبة لأجل العناية الواجبة/المراقبة المستمرة/التقييم المستمر للتعرض لمخاطر الاحتيال إلى مسؤول نشاط الأعمال (BAO).
 - 5- تتضمن العناية الواجبة نموذج تقييم تأثير الاحتيال من قبل طرف ثالث ("TP-FIAT")، والذي تم تصميمه لإجراء تقييمات التحكم في قدرات المورد فيما يتعلق بالتخفيف من مخاطر الاحتيال. يصف إجراء التشغيل هذا مجموعة من الخطوات التي يجب على مسؤول نشاط الأعمال (BAO) أو مسؤول الطرف الثالث (TPO) ومسؤول إدارة مخاطر الاحتيال ("FRMO") تنفيذها لتحديد وإدارة مخاطر الاحتيال.

- 3-8 يشمل الموردون المعرضون لمخاطر احتيال أعلى بطبيعة عملهم، على سبيل المثال لا الحصر:
 - 1- 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؛
 - 2- ومن لديهم اتصال بشبكات/أنظمة Citi؛
 - 3- ومن يقدمون أو يدعمون أو يمكنهم الوصول إلى الخدمات والإمكانات التي تكون مصدر استهداف لارتكاب الاحتيال أو تمكينه، بما في ذلك:

- (أ) طلبات تحديد هوية، أو التحاق بعمل، أو معالجة من عملاء جدد.
- (ب) أنشطة تحويل مدفوعات/أموال من Citi أو العملاء، و/أو مصادقة وصول عملاء Citi لهذه الخدمات؛
- (ج) إجراء تغييرات على بيانات Citi أو البيانات القائمة بين Citi والعملاء (مثل البيانات الديموغرافية) أو التحقق منها أو تنفيذها؛
- (د) توفير أدوات معاملات أو تقديم خدمات بشأنها أو مصادقتها (مثل بطاقات الخصم/الائتمان، المحافظ الإلكترونية، دفاتر الشيكات، وغيرها)؛
- (هـ) توفير أنشطة إدارة الاحتيال التشغيلية إلى Citi أو دعمها، والتي تختص بمنع حوادث الاحتيال أو اكتشافها أو الاستجابة لها؛

- (و) توفير الوصول المادي إلى النقد والصكوك المالية والأصول/السلع المادية؛
 (ز) الدخول دون مرافق أو خارج ساعات العمل إلى مرافق Citi؛
 (ح) البيانات المالية: أنشطة المحاسبة، مثل إضافة مدخلات إلى دفتر الأستاذ العام أو الفرعي (GL/SL)؛
 (ط) كسب أو إنفاق مكافآت للأنشطة المشمولة بالحوافز.

9 التفاعل مع وسائل الإعلام والظهور العام

إدارة الخدمات المؤسسية والشؤون العامة العالمية لدى Citi هي الإدارة الوحيدة المخولة بإصدار البيانات الصحفية أو التصريحات العامة نيابةً عن Citi. ولا يجوز للموردين إصدار أي بيان صحفي يُشير بشكل مباشر أو غير مباشر إلى Citi أو أي عقد أو اتفاقية بين أحد الموردين و Citi أو أي منتجات وخدمات يشتريها Citi من المورد. ولا يجوز للموردين الموافقة على أي أنشطة علاقات عامة فيما يخص Citi أو المشاركة فيها مع العملاء أو موظفي Citi أو مورديه الآخرين أو العملاء الآخرين للموردين أو أي أطراف ثالثة دون الحصول على موافقة كتابية مسبقة من جهة الاتصال الرئيسية للأعمال في Citi.

لا يجوز للموردين إعلان أو نشر أي مادة بصيغة خطية أو إلكترونية (بما في ذلك الكتب والمقالات وعمليات التدوين الصوتي وعمليات البث الشبكي والمدونات والموضوعات المحملة على مواقع الويب والصور ومقاطع الفيديو ووسائل الإعلام الاجتماعي وغيرها) أو ذكر اسم Citi أو عملياته أو عملائه أو منتجاته أو خدماته في أي لقاءات أو مقابلات أو في فعالية عامة دون الحصول على موافقة كتابية مسبقة من جهة الاتصال الرئيسية للأعمال في Citi والمسؤول الأول للشؤون العامة القطرية.

ولا يجوز للموردين، سواء فيما يتعلق بتقديم الخدمات أو المنتجات إلى Citi أو غير ذلك، استخدام الإشارات المميزة أو العلامات التجارية أو علامات الخدمة أو الأسماء التجارية أو الشعارات أو الرموز أو أسماء العلامات التجارية التي تخص Citi دون الحصول في كل حالة على موافقة كتابية مسبقة منه. لا يجوز للموردين استخدام اسم Citi أو شعاره أو علاماته التجارية أو منشأته أو علاقاته لتحقيق فائدة أو للعمل خارج Citi (بما في ذلك في ترويسات الخطابات أو مواقع الويب الشخصية أو المدونات أو مواقع شبكات التواصل الاجتماعي الأخرى). وعلاوة على ذلك، لا يجوز للموردين استخدام اسم Citi أو منشأته أو علاقاته للأغراض الخيرية أو التطوعية.

10 الاتصالات الإلكترونية المكتوبة

عند التعامل مع موظفي Citi أو عند تأدية التزاماتهم لصالح Citi أو نيابةً عنه، لا يُسمح للموردين إلا باستخدام معدات وأنظمة وخدمات الاتصالات الإلكترونية المعتمدة من جانب Citi. يجب الموافقة على قنوات الاتصالات الإلكترونية الجديدة أو الموسعة أو المعدلة لدى Citi، سواء كأدوات مستقلة أو مدمجة في منصة أوسع يوفرها Citi أو يوفرها طرف ثالث وفقاً لمتطلبات Citi المعمول بها، أو التي تم إخطار المورد بها كتابةً من جانب BAO. يحظر إجراء مراسلات بين شركات أعمال Citi وموظفي Citi عبر منصات مراسلات غير التي يعتمد عليها Citi مثل WhatsApp و WeChat LINE و Slack و Signal و Telegram و iMessage و SMS و Viber 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 نزلتها أو خزنتها أو نقلتها أو استقبلتها أو حذفها معدات وأنظمة وخدمات الاتصالات التي يوفرها Citi. ويجوز لـ Citi مراقبة معدات وأنظمة وخدمات الاتصالات الإلكترونية، فضلاً عن الاتصالات الإلكترونية نفسها. فهذه الاتصالات الإلكترونية تخضع لملكية Citi ويجوز الاحتفاظ بها وفقاً لمتطلبات الاحتفاظ بالسجلات المعمول بها (وفقاً للقانون واللوائح المحلية).

<https://policydirectory.citi.net/cpd/layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 الأنشطة والمساهمات السياسية

تنظم مجموعة متنوعة من القوانين، مثل تلك المتعلقة بما يلي: التأثير الأجنبي؛ وتمويل الحملات الانتخابية؛ والهدايا والترفيه؛ والضغط التشريعي والشعبي والضغط من أجل كسب النوايا الحسنة والضغط التنظيمي؛ والمشتريات، والرشوة مقابل النفوذ؛

والأوراق المالية، والأنشطة السياسية والإفصاحات المتعلقة بهذه الأنشطة، سواء من جانب Citi أو مورديه. ويحظر على الموردين مزاوله أي نشاط سياسي لا يمثل لسياسة أو معايير Citi ذات الصلة أو القانون أو اللوائح المعمول بها.

يشمل النشاط السياسي على سبيل المثال لا الحصر:

- 1- 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 يخوض حملة انتخابية لتولي منصب عام أو لجنة حزب سياسي أو لجنة سياسية؛
- 2- أو المشاركة في أنشطة كسب تأييد أو دعاية لمسؤولين حكوميين، سواء كان بشكل مباشر أو من خلال أطراف ثالثة، بما في ذلك محاولات التأثير على المسؤولين والتشريعات والتي قد تشمل، حسب الاختصاص القضائي، محاولات التأثير على وضع قواعد الوكالة أو ترسية عقود حكومية؛
- 3- أو السعي إلى تولي منصب سياسي مرتبط بالحكومة أو قبوله أو شغله، 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 يزعم أنه نيابةً عن) Citi، أو عملائه، دون الحصول على تصريح كتابي مسبق من مكتب مراقبة العمليات العالمية للشؤون الحكومية لدى Citi من خلال ggacontrol@citi.com. ورغم أن Citi قد يدفع رسوم و/أو يسدد تكاليف عينية لخدمات الأنشطة السياسية المتعاقد عليها والمسموح بها التي يقدمها المورّد، مثل ممارسات الضغط، فإن Citi لن يعوض مطلقاً أي مورّد أو أي من موظفيه عن أي من المساهمات السياسية الشخصية أو المؤسسية أيًا كان نوعها.

12 مكافحة غسل الأموال ("AML")

ينطبق هذا على الموردين الذين يؤدون خدمات معينة تتعلق بالعملاء (مثل إجراءات التسجيل، وفحص حسابات العملاء والمعاملات) أو تسليم البيانات/المقاييس المتعلقة بالأنشطة السابقة؛ و/أو العمل كوسيط فيما يتعلق بالمعاملات أو الأدوات المالية (مثل خدمات الإيداع عن بعد، وخدمات البريد السريع، وخدمات السيارات المصفحة، وخدمات الصناديق الآمنة، والتحويلات الإلكترونية، والأصول الرقمية).

1-12 التزامات TTS:

1- الامتثال لعمليات Citi والقوانين المعمول بها:

- الحفاظ على عمليات وإجراءات Citi والامتثال لها والتي تكون مُخصصة لتلبية متطلبات القوانين المعمول بها والامتثال لها، وتشمل (1) قانون جرام-ليش-بليلي 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. ستتناول هذه السياسات والإجراءات أدوار ومسؤوليات مكافحة غسل الأموال، بما في ذلك متطلبات الإبلاغ الفوري عن أي نشاط تتم ملاحظته يبدو غير عادي أو يحتمل أن يكون غير عادي فيما يتعلق بالأنشطة المالية والمعاملات واستلام النقد.

2- التدريب السنوي وعناصر البرنامج الخاصة بالموظفين:

- ضمان حصول الموظفين الذين يقدمون الخدمات إلى Citi على تدريب سنوي فيما يخص الأدوار والمسؤوليات التي تتعلق بمكافحة غسل الأموال، بما في ذلك متطلبات الإبلاغ الفوري عن أي نشاط تتم ملاحظته يبدو غير عادي أو يحتمل أن يكون غير عادي فيما يتعلق بالأنشطة المالية والمعاملات واستلام النقد. ويشمل التدريب، على سبيل المثال لا الحصر، المكونات التالية:
- أ- الإبلاغ عن أي نشاط مشبوه وتصعيده.

- ب- برنامج "KYC" (Know Your Customer)، ويشمل برنامج Customer Identification Program (CIP)، وفحص العقوبات والأسماء، والعناية الواجبة تجاه العميل (CDD)، والعناية الواجبة المعززة (EDD)، وتحديد الملاك المستفيدين النهائيون (UBOs).
- ج- مراقبة المعاملات عبر جميع الأدوات والأنشطة المالية ذات الصلة.
- د- عمليات الإبلاغ/القياسات الدورية، بما في ذلك الإبلاغ عن التغييرات القانونية والتنظيمية والتغييرات الجوهرية في برنامج AML.
- هـ- الاختبارات وضوابط مدى فعالية برنامج AML، بما في ذلك زيارات الموقع.

3- الامتثال لأحكام العقد:

- الامتثال لأي أحكام تعاقدية تحدد أي برنامج يجب أن يضعه المورد.
- 4- الإبلاغ الفوري عن الانتهاكات المشتبه بها:
 - إبلاغ Citi كتابيًا على الفور عن أي انتهاكات مشتبه بها للقانون، بما في ذلك أي نشاط يتم رصده ويوحى بممارسات غير اعتيادية أو يُحتمل كونها غير اعتيادية ذات صلة بتدفق النقد أو الأنشطة المالية أو المعاملات التي تضم Citi أو عملاءه.

5- منع التهرب الضريبي والإبلاغ عنه:

- الامتثال لقوانين ولوائح الضرائب المعمول بها في البلدان التي يعملون فيها.
- ولا ينبغي بأي حال من الأحوال أن يتورط الموردون في التهرب الضريبي المتعمد غير المشروع أو تسهيل هذا التهرب نيابة 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 الموردون إجراءات وقائية معقولة ذات صلة بالتهرب الضريبي وأن يبلغوا Citi كتابةً وفورًا بأي انتهاكات فعلية أو مشتبه فيها بخصوص Citi.

2-12 السياسات والإجراءات الداخلية للموردين:

يجب على الموردين وضع سياسات وإجراءات داخلية مناسبة للامتثال لجميع قوانين ولوائح AML السارية حاليًا أو التي ستدخل حيز التنفيذ لاحقًا.

13 إدارة السجلات

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

يطلب Citi من جميع الموردين الذين بعهدتهم معلومات تخص Citi التعاون مع مسؤول نشاط الأعمال ("BAO") ذوي الصلة بهم أو جهة الاتصال الرئيسية للأعمال في Citi من أجل (1) تحديد وتصنيف المعلومات كسجلات أو معلومات مؤقتة لأغراض إدارة السجلات التي تخص Citi؛ (2) وتصنيف السجلات وفقًا إلى Master Record Catalogue ("MRC") لدى Citi؛ (3) والاحتفاظ بالمعلومات استنادًا إلى متطلبات الاحتفاظ لدى Citi؛ (4) وفي حالة عدم وجود أمر احتفاظ بالمعلومات، التخلص من المعلومات بشكل مناسب في نهاية دورة حياة تلك المعلومات.

يجب أن يعمل BAO أو جهة الاتصال الرئيسية للأعمال في Citi مع المورد لضمان أن المورد قد قام بتحديد وتصنيف السجلات وفقًا لرموز سجلات Citi في MRC وأنه يتم تحديث المخزون بشكل سنوي على الأقل. ويلتزم المورد بالتقيد بمتطلبات إدارة السجلات التي يتم إبلاغه بها من جانب مسؤول نشاط الأعمال (BAO). السجلات التي تستوفي معايير

الأهلية للتخلص منها يجب أن يتم التخلص منها بالشكل الملائم في أسرع وقت ممكن، على ألا يتجاوز ذلك ستة أشهر بعد استيفاء متطلبات الاحتفاظ، ما لم تكن خاضعة لأوامر الاحتفاظ بالمعلومات. ويجب إتلاف المعلومات المؤقتة في موعد أقصاه عامين من آخر استخدام لها، ما لم تخضع لأوامر الاحتفاظ بالمعلومات. المعلومات المؤقتة التي تتضمن معلومات شخصية، يجب حذفها بمجرد تلبية الغرض الذي تم جمعها من أجله، ما لم تخضع لأوامر الاحتفاظ بالمعلومات. يجب على المورد التوقف عن إتلاف معلومات Citi أو تغييرها عند إخطاره بوجود أمر للاحتفاظ بالمعلومات. يقوم المورد بمراجعة جهة الاتصال الرئيسية للأعمال في Citi أو مسؤول نشاط الأعمال (BAO) في حالة عدم التيقن.

تتم مراجعة وتحديث قواعد الاحتفاظ المدرجة في جداول الاحتفاظ القطرية حسب الحاجة لتكون متوافقة مع التغييرات التنظيمية والداخلية من جانب DRIM، وذلك على أساس ربع سنوي. في حالة وجود أي تغيير يؤثر على المورد، فسوف يقوم BAO بإخطار المورد بذلك. يجب على المورد تقييم الأثر وتنفيذ التغييرات في الأنظمة والعمليات وعمليات الجرد ذات الصلة، وأنواع السجلات التي يمتلكها ويديرها في غضون 90 يومًا من تاريخ الإخطار من BAO.

يتحمل الموردون 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 نشاط الأعمال (BAO). يجب على المورد، عند الطلب، إعادة معلومات Citi على النحو المطلوب بموجب الشروط التعاقدية المعمول بها. يجب على الموردين عدم التخلص من أي من معلومات Citi، بغض النظر عن تصنيفها (سواء كانت سرية أو غير سرية) دون الحصول على موافقة جهة الاتصال الرئيسية للأعمال في Citi أو BAO، والتي يجب أن تتضمن التأكيد على عدم وجود أي أمر احتفاظ بشأن المعلومات التي سيتم التخلص منها. إن متطلبات إدارة السجلات والاحتفاظ بها وجميع متطلبات مناوله المعلومات الأخرى تظل سارية بعد إنهاء العقد أو انتهائه ما لم يتم الاتفاق صراحةً على غير ذلك.

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

14 مرونة المؤسسة/استمرارية الأعمال

تتطبق هذا على الموردين الذين يقدمون الخدمات أو يستضيفون البنية التحتية التكنولوجية/التطبيقات التي يستخدمها Citi. يتحمل مسؤول نشاط الأعمال (BAO) في Citi مسؤولية إبلاغ المورد بمتطلبات التطبيق واستمرارية العمل (COB).

1-14 موارد الاسترداد

يجب أن توفر خطة التعافي من الكوارث الخاصة بالمورد موارد بديلة لديها القدرة على تقديم جميع المنتجات والخدمات إلى Citi في حالة تعطيل المواقع الرئيسية للمورد. ويجب أن تكون موارد الاسترداد في مواقع منفصلة جغرافيًا عن المواقع الرئيسية بفواصل كافٍ لتقليل أو القضاء على التهديد المتمثل في إمكانية تأثير نفس الحدث الكارثي على كلٍ من المواقع الرئيسية ومواقع الاسترداد.

- 1- لا 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- يجوز لموردي التطبيقات تنفيذ نوع Hot/Hot من البنية المعمارية لضمان تكوين توفر عالٍ (HA). وتتطلب هذه البنية المعمارية وجود نظامين (على الأقل) متطابقين في التكوين وجاهزين للتشغيل ومتاحين للعملاء/المستخدمين. الميزة الأكثر أهمية التي يقدمها هذا النموذج هي أن البنية/البيئات البديلة تعمل بالتزامن مع مركز البيانات (الإنتاج) الأساسي.

2-14 مستويات خدمات الاسترداد

يجب أن تلي خطة استمرارية الأعمال الخاصة بالموردين مستويات الخدمة المحددة حتى تكون فعالة بالنسبة إلى Citi. كحد أدنى، يجب أن تحدد خطة التعافي من الكوارث الخاصة بالمورد قيمًا محددة لكلٍ من:

- 1- هدف وقت الاسترداد

- 2 هدف نقطة الاسترداد
- 3 موارد التعافي/القدرة التكنولوجية
- 4 مدة الاسترداد

3-14 خطة التعافي من الكوارث

يضع المورد خطة للتعافي من الكوارث لأجل استمرارية الأعمال (ويقدم الأدلة على اختباراته الحالية والدورية لتلك الخطة إذا طلب Citi ذلك) وبحيث يتمكن المورد، في حال حدوث أي اضطراب في قدرة المورد على توفير المنتجات/الخدمات أو أداء الالتزامات الأخرى بموجب هذه الاتفاقية من أي موقع معين أو من خلال جهود أي أفراد معينين، من القيام على الفور بتوفير المنتجات/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 والمورد، وبصفة سنوية بعد ذلك، طالما كان كل أمر عمل ساري المفعول. يزود المورد Citi بأي تعليمات أو معلومات أخرى ضرورية كي يواصل Citi تلقي المنتجات/الخدمات من المورد في ظل الظروف التي يقوم المورد فيها باستدعاء خطة التعافي من الكوارث الخاصة به. يقر المورد ويضمن ويتعهد بأن خطته للتعافي من الكوارث سوف تشمل، على الأقل، ما يلي:

- 1- إجراءات واستراتيجيات الاسترداد، بما في ذلك الانتقال و/أو نقل العمل و/أو الوصول عن بعد للتخفيف من آثار تعطل العمليات بما في ذلك عدم إتاحة التكنولوجيا (رفض الخدمة/DoS)، وعدم إتاحة موقع العمل الأساسي (رفض الوصول/DoA)، وعدم إتاحة الموظفين (بما في ذلك المقاولين من الباطن)؛
- 2- صيانة المورد (وتشمل على سبيل المثال لا الحصر) لموقع ثانوي للتعافي من الكوارث منفصل عن مواقع المنتج/الخدمة، واستخدام خطوط وخوادم اتصالات إضافية؛
- 3- إجراءات النسخ الاحتياطي/استعادة تشغيل المنتجات/الخدمات المستضافة وتطبيقها، بما في ذلك خطة مفصلة وموثقة للاستجابة للانقطاع المطول في المنتجات/الخدمات الناتج عن انقطاع التيار الكهربائي أو تعطل النظام أو الكوارث الطبيعية أو غيرها من الظروف غير المتوقعة التي تتضمن العمليات والإجراءات الخاصة باستئناف العمليات في غضون فترة زمنية يتفق عليها الطرفان؛
- 4- إجراءات حماية جميع المحتوى؛
- 5- الإجراءات وأي اتفاقيات مع طرف ثالث لاستبدال المعدات (مثل معدات الكمبيوتر)؛
- 6- الإجراءات الخاصة بأي منشآت إنتاج خارج الموقع؛
- 7- سوف تنص خطة التعافي من الكوارث الخاصة بالمورد على ما يلي:

- أ) سوف يقوم المورد على الفور بإخطار Citi بأي كارثة يمكن أن تؤثر سلباً على المنتجات/الخدمات؛
- ب) سوف يمد المورد Citi، في غضون 24 ساعة من الإشعار المذكور، بخطة لمواصلة تقديم المنتجات/الخدمات في منشأة معالجة بديلة؛
- ج) يجب أن تكون المنتجات/الخدمات جاهزة للعمل بشكل كامل ضمن هدف وقت الاسترداد (RTO)، وأن يبلغ (RTO)، في حالة عدم النص على خلاف ذلك في العقد المعمول به، 4 ساعات أو أقل بالنسبة لتلك العمليات التي صنفها Citi بدرجة أهمية "حرجية للمؤسسة" أو "مرتفعة"، و 24 ساعة أو أقل لتلك العمليات التي صنفها Citi بدرجة أهمية "متوسطة"، و 72 ساعة أو أقل لتلك العمليات التي صنفها Citi بدرجة أهمية "منخفضة"؛ و
- د) في حالة تعطل أجزاء من منشآت المورد، سيعامل المورد Citi على نحو لا يقل تفضيلاً عن معاملة المورد لعملائه التجاريين الآخرين.

4-14 متطلبات خطة التعافي من الكوارث المطبقة على الخدمات المستضافة

إلى حد قيام المورد بإدارة وتوفير خدمة مستضافة إلى Citi، يجب أن تطبق كذلك الأحكام التالية. سوف تتضمن خطة التعافي من الكوارث على الأقل ما يلي:

- 1- 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؛

- 2- وإضافةً لذلك، ستتص خطة التعافي من الكوارث الخاصة بالمورد على ما يلي: (أ) أن يخطر المورد Citi كتابياً في غضون ساعتين (2) من حدوث أي كارثة يمكن أن تؤثر سلباً على الخدمات المستضافة؛ (ب) أن يقدم المورد إلى 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؛
- 3- يوافق المورد، عند الطلب، على إصدار المعلومات اللازمة التي تتيح إلى Citi وضع خطة للتعافي من الكوارث وخطة لاستمرارية الأعمال والتي ستعمل بالتنسيق مع خطة التعافي من الكوارث وخطة استمرارية الأعمال المطبقة لدى المورد؛ و
- 4- في حالة تعطل أجزاء من منشآت المورد، سيعامل المورد Citi على نحو لا يقل تفضيلاً عن معاملة المورد لعملائه التجاريين الآخرين.

5-14 التغييرات في خطة التعافي من الكوارث

يجوز أن يقوم المورد بتغيير خطة التعافي من الكوارث الخاصة به طالما أن التغييرات لا تؤدي إلى تدهور خطة التعافي من الكوارث بطريقة من المحتمل أن تؤثر سلباً على الخدمات (مثل إطالة أهداف وقت الاسترداد (RTO) الخاصة بها). يلتزم المورد بأن يبلغ Citi على الفور بأي تغييرات تطرأ على خطة التعافي من الكوارث، ويقوم، بناءً على طلب Citi، بشرح التغييرات حتى يفهم العميل التغييرات تماماً ويكون قادراً على الاستجابة لها.

6-14 خطة التعافي من الكوارث للمقاولين من الباطن

يلتزم المورد بأن يضمن أن يكون لدى أي مقاول من الباطن تابع للمورد خطة للتعافي من الكوارث وضوابط بشأن استمرارية الأعمال ذات الصلة بما يتوافق مع متطلبات Citi للموردين. يجب على المورد توفير الرقابة المناسبة على المقاولين من الباطن، بما في ذلك المراجعة الدورية لهذه الضوابط ونتائج الاختبار، وضمان معالجة أي ثغرات يتم تحديدها في الوقت المناسب.

7-14 استدعاء خطة التعافي من الكوارث والإخطار بالآزمات

- يقوم المورد على الفور بإخطار جهة الاتصال الرئيسية للأعمال في Citi:
- 1- عندما يستدعي المورد خطة التعافي من الكوارث الخاصة به؛ و
 - 2- بشأن أي أزمة أو تهديد أو حدث إلكتروني ضد المورد أو مقاوليه من الباطن بحيث يُحتمل إلى حد معقول أن يكون له تأثير سلبي على الخدمات أو المنتجات المقدمة إلى Citi.

8-14 الاختبار

يجب اختبار جميع موارد وخطط التعافي الخاصة بالمورد في غضون 120 يوماً عقب تنفيذ الإنتاج (90 يوماً في حالة التطبيقات التي صنفها Citi بدرجة أهمية "حرجة للمؤسسة")، ويجب اختبارها سنوياً (كل 12 شهراً) على الأقل. ويجب أن يبين الاختبار قدرة المورد على تلبية مستويات الخدمة المتعلقة بالتعافي لجميع المنتجات والخدمات المقدمة إلى Citi. يجب أن تكون هذه الاختبارات شاملة وتتضمن النطاق الكامل للخدمات المقدمة إلى Citi. يجب أن يرسل الموردون إلى Citi إخطاراً مقدماً قبل 30 يوماً تقويمياً على الأقل من إجراء الاختبار الخاص باسترداد المنتجات والخدمات المقدمة إلى Citi. ويجوز لـ Citi المشاركة في اختبارات الاسترداد الخاصة بالمورد أو مراقبتها والتي يستخدمها Citi للتحقق من وظائف العمل الخاصة بالتطبيق في بيئة الاسترداد. إذا رغب Citi في المشاركة، فسيقوم المورد 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 المورد إلى Citi ملخصاً لأهداف الاختبار وخطة الاختبار ونتائج الاختبار، بما في ذلك الأطر الزمنية المطلوبة للاسترداد والأدلة على نتائج الاختبار (مثل لقطات الشاشة).

9-14 التحقق من الحجم

يجب على المورد الذي يستضيف التطبيقات المصنفة من قبل Citi بدرجة أهمية حرجة للمؤسسة أن يثبت أنه يمكن معالجة أحجام الإنتاج في بيئة COB/التعافي من الكوارث. يجب أن يتم الاتفاق بين Citi والمورد على المنهجية المفترض استخدامها لإجراء عملية التحقق.

10-14 استخدام أنظمة Citi لتقديم الخدمات

بناءً على طلب Citi أو شركات Citi التابعة، فسوف يشارك الموردون الذين يستخدمون أنظمة Citi في تدريبات التعافي من الكوارث التي يجريها Citi بدون تكلفة أو رسوم من Citi.

11-14 معالجة نتائج الاختبارات

إذا أظهرت أي من نتائج اختبارات المورد فشلاً في تحقيق أي هدف من أهداف الاختبار أو أي هدف من أهداف وقت الاسترداد (RTO) المعمول بها، سوف يقوم المورد بتنفيذ تحليل لسبب المصدر ويقوم بمعالجة أي مواطن قصور يتم تحديدها فوراً. بعد تنفيذ ذلك الإصلاح، يقوم المورد بإجراء إعادة اختبار في موعد لا يتجاوز مائة وعشرين (120) يوماً تقويمياً (90 يوماً تقويمياً في حالة التطبيقات التي صنفها Citi بدرجة أهمية "حرجة للمؤسسة") عقب فشل الاختبار الأولي (أو الفترة الزمنية المحددة في أمر العمل ذي الصلة).

12-14 إدارة الأزمات

بالنظر مع خطة استمرارية الأعمال، يجب على المورد وضع خطة لإدارة الأزمات تُعنى بقيادة عمليات التعافي والسيطرة عليها. وعلى أقل تقدير، يجب أن تحدد خطة المورد لإدارة الأزمات أشخاصاً محددين يتمتعون بالسلطة الكافية لتنفيذ عملية التعافي، وتحديد بروتوكولات الاتصال والتصعيد لجمع المعلومات المتعلقة بالأزمات ونشرها، وتضمين بروتوكولات الإخطار والتصعيد للتواصل مع Citi في حالة وقوع أي أزمة.

13-14 تقييمات استمرارية الأعمال

يخضع الموردون لعملية تقييم استمرارية الأعمال (CoB) للأطراف الخارجية لدى Citi لتقييم سياسات المورد وإجراءاتهم وضوابطهم فيما يتعلق بالامتثال لمتطلبات Citi وأي متطلبات قانونية و/أو تنظيمية (منطقة على Citi أو على المورد) تتعلق باستمرارية الأعمال. ويتكون التقييم من استبيانات تتطلب إجابات من المورد مشفوعة بالأدلة الداعمة، ويمكن أن تتضمن زيارات إلى مواقع المورد. وإذا ما كشفت النتائج التي توصل إليها التقييم عن وجود مشكلات أو مخاوف أو أشارت إلى وجودها، فسيحرص Citi على توثيق النتائج ويعمل مع المورد لتحديد الوسائل اللازمة لتصحيح هذه المشكلات. يجب على الموردين إجراء التصحيحات اللازمة على وجه السرعة و/أو إضافة ضوابط تعويضية لمعالجة مخاوف Citi على النحو المرضي لـ Citi بشكل معقول.

14-14 المرونة التشغيلية

خدمات الأعمال الحرجة هي تلك الخدمات التي قد يؤدي توقف تقديمها إلى إحداث تأثير سلبي كبير على Citi أو عملائه أو على النظام المالي. يجب على المورد ضمان عدم تجاوز أي انقطاع في تقديم عناصر الخدمات التي ترقى إلى مستوى خدمات الأعمال الحرجة أو تدعم تقديم Citi لخدمات الأعمال الحرجة، أو تدعم تقديم خدمات الأعمال الحرجة من جانب Citi، على النحو الذي حدده Citi من وقت لآخر (يشار إليها باسم "خدمات الأعمال الحرجة") المدة التي حددها Citi، أو عدم انتهاك أي مقياس ذي صلة يحدده Citi ("درجات تحمل الأثر") حسبما يتم إخطار المورد به من وقت لآخر. سيتم التعبير عن "درجات تحمل الأثر" كمقياس زمني واضح يعادل مقدار الوقت الذي قد ينقطع فيه تقديم الخدمة. ويتعين على Citi والمورد مراجعة "درجات تحمل الأثر" سنوياً كجزء من عملية حوكمة العقود المستمرة. عندما يُطلب من Citi تعيين أكثر من "درجة تحمل أثر" واحدة لخدمة فردية من خدمات الأعمال الحرجة وفاءً بمتطلبات أكثر من هيئة تنظيمية واحدة، فقد يحدد Citi عندئذٍ "درجات تحمل أثر" منفصلة لخدمة الأعمال الحرجة هذه. يجب على المورد:

- 1- إخطار Citi بمجرد أن يصل إلى علمه أنه فشل (أو من المحتمل بشكل معقول أن يفشل) في تقديم أي خدمة ضمن نطاق (درجة/درجات تحمل الأثر) المقابل الذي حدده Citi جنباً إلى جنب مع شرح لأسباب أي فشل محتمل أو فشل فعلي والخطوات التي يتم اتخاذها للتخفيف من أثر ذلك الفشل؛
- 2- عند طلب القيام بذلك، تقديم مساعدة معقولة إلى Citi لتمكينه من تحديد الأشخاص والعمليات والتقنيات والمرافق والمعلومات اللازمة للمورد لتقديم الخدمة التي تدعم خدمات الأعمال الحرجة؛
- 3- تقديم المساعدة المعقولة إلى Citi لتمكين Citi من إجراء:

(أ) أي اختبار سيناريو داخلي لقدرة المورد على البقاء ضمن نطاق (درجة/درجات تحمل الأثر) لكل خدمة أعمال حرجة في حالة حدوث توقف شديد ولكنه معقول في عمليات Citi أو عمليات المورد؛

(ب) وأي دروس مستفادة تتم ممارستها بعد اختبار السيناريو لتمكين Citi من تحديد نقاط الضعف وأي إجراءات ضرورية لتحسين قدرة المورد على الاستجابة بفعالية والتعافي من الاضطرابات

المستقبلية.

عندما يحدد أي اختبار سيناريو داخلي من قبل Citi نقاط الضعف أو القيود المفروضة على قدرة المورد على تقديم خدمات ضمن درجة/درجات تحمل الأثر المقابلة التي حددها Citi وبعد أي فشل من جانب المورد في تقديم أي خدمة ضمن نطاق (درجة/درجات تحمل الأثر) المقابل الذي حدده Citi، يوافق الطرفان على خطة (بما في ذلك جدول زمني لتنفيذ الخطة) لضمان أن يتخذ المورد 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 عملياً.

15-14 ترتيبات الضمان

بناءً على طلب Citi، يجب على الموردين (1) الذين يرخصون البرامج لـ Citi للتشغيل ضمن بيئة Citi أو (2) الذين يقدمون خدمة مستضافة لـ Citi، التأكد من أن المواد المودعة يتم إيداعها لدى وكيل الضمان المعين لدى Citi، كما يجب عليهم تنفيذ جدول تسجيل المودع أو النماذج الأخرى المطلوبة من قبل وكيل الضمان فيما يتعلق بمواد الإيداع بموجب اتفاقية الضمان المعمول بها. بعد ذلك، وعلى مدار الفترة المتبقية من أجل الاتفاقية المعمول بها فيما يتعلق بالترخيص أو الخدمة المستضافة، سوف يقوم المورد بإيداع إصدارات محدثة من مواد الإيداع لدى وكيل الضمان للتأكد من أن كود المصدر معلق التسليم ومواد الإيداع الأخرى المودعة معلقة التسليم تظل محدثة وفق أحدث إصدار من البرنامج المطبق على إصدار البرنامج أو الخدمات المستضافة التي يستخدمها Citi. ويتم تسليم تحديثات (تحديثات) للبرنامج المرخص لـ Citi أو التعديلات على الضمان في غضون ثلاثين (30) يوماً من تاريخ أي تحديث (تحديثات) للبرنامج المرخص لـ Citi أو التعديلات على الخدمات المستضافة التي يستخدمها Citi. سوف يلتزم المورد التزاماً كاملاً بجميع التزامات ومتطلبات المودع كما هو منصوص عليه في اتفاقية الضمان. يقع على عاتق المورد وحده مسؤولية جميع تكاليف ورسوم الضمان، بما في ذلك، على سبيل المثال لا الحصر، رسوم الإعداد، والرسوم السنوية، ورسوم الإيداع، ورسوم الخدمات، وأي رسوم وتكاليف ضمان أخرى. في حالة حدوث حدث إصدار، يقوم وكيل الضمان بإصدار مواد الإيداع إلى Citi أو من يعينه Citi نيابة عنه، وفقاً لشروط الاتفاقية الأساسية واتفاقية الضمان.

في حالة تسليم الكود المصدر (أو مواد الإيداع الأخرى) إلى Citi أو إلى من يعينه Citi نيابة عنه (سواء بشكل مباشر من قبل المورد أو من قبل وكيل الضمان تنفيذاً لالتزاماته بموجب اتفاقية الضمان المعمول بها)، فإن الكود المصدر ومواد الإيداع تخضع للترخيص الحالي بموجب الاتفاقية ذات الصلة الموقعة بين المورد و Citi؛ شريطة أن يُعتبر كل ترخيص بأنه يعطي الحق لـ Citi في استخدام وتعديل الكود المصدر ومواد الإيداع الأخرى حسب الضرورة المعقولة لأجل: (1) دمج وضمان توافق، البرنامج ومواد الإيداع الأخرى مع أنظمة Citi؛ (2) وجعل البرنامج أو مواد الإيداع الأخرى متوافقة مع القانون المعمول به أو معايير الصناعة أو ممارسات السوق؛ (3) وتمكين البرنامج أو مواد الإيداع الأخرى كي تظل محدثة وفق أحدث الابتكارات التكنولوجية؛ (4) وتمكين البرنامج ومواد الإيداع الأخرى من تحقيق أغراض أعمال Citi والشركات التابعة له ضمن نطاق الترخيص الحالي. تخضع أي إصدارات من البرنامج تتضمن تعديلاً تم تطويره بواسطة Citi أو نيابة عن Citi باستخدام الكود المصدري لجميع أحكام هذا القسم والاتفاقية الأساسية؛ إلا إنه يراعى ألا يكون للمورد أي حق أو ملكية أو مصلحة في أي تعديلات، وتؤول جميع حقوق الملكية الفكرية في أي تعديلات بشكل حصري إلى Citi.

سوف يبذل المورد جهوداً معقولة من الناحية التجارية مع الأطراف الثالثة التي قدمت أي برنامج تم استخدامه في البرنامج للسماح للمورد بوضع الكود المصدر لذلك البرنامج الخاص بالطرف الثالث في إيداع الكود المصدر. في حال رفض الطرف الثالث منح المورد هذا الحق، يلتزم المورد عندئذ ببذل جهود معقولة من الناحية التجارية لجعل اتفاقية ترخيص البرنامج الخاصة بالطرف الثالث قابلة للتحويل إلى Citi في حالة وقوع حدث إصدار.

يخضع الكود المصدر الذي يتم تسليمه إلى Citi وفقاً لهذا القسم للترخيص الحالي للبرنامج المرخص أو الخدمات المستضافة ذات الصلة، شريطة أنه يجوز لـ Citi استخدام وتعديل الكود المصدر والبرنامج فيما يتصل بمتطلباته التجارية والتشغيلية، بما يوفر الفرصة لأن يظل البرنامج مواكباً للابتكارات التكنولوجية، وأن يمثل للقانون المعمول به. تخضع أي إصدارات من البرنامج تتضمن تعديلاً تم تطويره بواسطة Citi أو نيابة عن Citi باستخدام كود المصدر لجميع أحكام الاتفاقية ذات الصلة؛ إلا إنه يراعى ألا يكون للمورد أي حق أو ملكية أو مصلحة في أي تعديلات، وتؤول جميع حقوق الملكية الفكرية في أي تعديلات بشكل حصري إلى Citi.

15 المعايير العالمية لفحص الخلفية الأمنية

تنطبق على جميع الموردين الخارجيين الذين يقدمون الخدمات إلى Citi.

1-15 نظرة عامة - فحص الخلفية الأمنية

يجب إجراء فحص الخلفية الأمنية وفقاً لجميع القوانين واللوائح المحلية المعمول بها. يجب على ممثلي المورد وموظفي المورد والمقاولين من الباطن، حسب الاقتضاء، تقديم جميع المعلومات والإفصاحات الذاتية الموضحة في هذه الوثيقة. وقد يُشكل تزييف المعلومات أو إغفالها سواء في السيرة الذاتية أو أثناء المقابلة الشخصية أو في أي من نماذج الالتحاق بالعمل أو أثناء عملية الالتحاق بالعمل، بصرف النظر عن وقت اكتشاف ذلك التزييف أو الإغفال، سبباً لرفض أو إنهاء التكليف لدى Citi وفقاً للقانون المحلي. وقد تُشكل أيضاً النتائج السلبية لأي عملية فحص يتم إجراؤها، بصرف النظر عن وقت اكتشافها، سبباً لرفض أو إنهاء التكليف لدى Citi وفقاً للقانون المحلي.

يمكن الاطلاع على معلومات إضافية حول إتمام فحص الخلفية الأمنية على هذا الرابط https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

2-15 جمع المعلومات الأساسية والتحقق من الهوية

قبل أن يبدأ أي موظف من موظفي المورد في القيام بأي مهمة لدى Citi، يجب على الموردين جمع الاسمين الأول والأخير للموظف والعنوان البريدي والعنوان الدائم (إذا كان مختلفاً) ورقم الهاتف وعنوان البريد الإلكتروني (إن وجد). كما يجب على موظفي المورد تقديم وثائق تثبت هويتهم. وقد يتضمن ذلك تقديم معلومات و/أو وثائق خاصة برقم الهوية الوطنية أو بطاقة هوية صادرة عن الحكومة ملصق بها صورة شخصية أو جواز سفر.

3-15 فحص العقوبات

إن جميع موظفي المورد الذين يؤدون العمل نيابة عن Citi، أو أي مالك يمتلك 25% أو أكثر من ملكية أحد موردي Citi بما في ذلك المقاولين من الباطن بغض النظر عن إمكانية الوصول إلى بيانات/أنظمة/شبكات Citi و/أو الوصول إلى مباني Citi، ينبغي أن يخضعوا للفحص في ضوء قائمة المواطنين المحددة أسماؤهم بصفة خاصة (SDN) والأشخاص المحظورين الصادرة عن مكتب مراقبة الأصول الأجنبية (OFAC) التابع لوزارة الخزانة الأمريكية؛ وكذلك في ضوء قائمة المناطق والاختصاصات القضائية الخاضعة لعقوبات مفروضة عليها من جانب الولايات المتحدة (يُشار إليها باسم "العقوبات الأمريكية")؛ بالإضافة إلى أي قائمة صادرة وأسماء الولايات القضائية الخاضعة لعقوبات مفروضة عليها من جانب سلطات خارج الولايات المتحدة، بما في ذلك قائمة العقوبات المالية الموحدة للاتحاد الأوروبي (EU)، والقائمة الموحدة الصادرة عن مجلس الأمن التابعة للأمم المتحدة (UN)، وقائمة عقوبات المملكة المتحدة (UK)، والقوائم الصادرة وفقاً للقوانين واللوائح المطبقة على الولاية القضائية المحلية (يُشار إليها باسم "العقوبات غير الأمريكية").

تتوفر القوائم الصادرة عن مكتب OFAC للجمهور العام في هذا الموقع الإلكتروني: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

4-15 الامتثال لقوانين الهجرة

يجب على المورد إثبات تبنيه لمجموعة من البروتوكولات وتنفيذها للتحقق من أن جميع الموظفين مصرح لهم بالعمل في البلدان التي يكلفون بالعمل بها. علاوة على ذلك، يجب على المورد: (1) التأكد من أن جميع الموظفين مصرح لهم بالعمل، (2) والالتزام بجميع القوانين واللوائح والسياسات المعمول بها (بما في ذلك متطلبات أهلية العمل والتحقق منها). كما يجب على المورد إثبات تطبيق بروتوكولات تهدف إلى ضمان امتثال موظفيه لجميع قوانين ولوائح الهجرة المعمول بها، والحفاظ على هذه البروتوكولات، والتأكد من أن موظفيه يحملون الوضع/تصنيف التأشيرة المناسب للمهام والأنشطة التي يضطلعون بها.

5-15 السجل الوظيفي

يجب على الموردين التحقق من السجل الوظيفي لموظفيهم على مدار السبع (7) أو العشر (10) سنوات الماضية إذا لزم الأمر وفقاً للأنظمة واللوائح المحلية. يجب التحقق من السجل الوظيفي لأي موظف لضمان أنه تم تمثيل أصحاب العمل والمناصب والتواريخ والواجبات على نحو دقيق. يجب على موظفي المورد أيضاً الإفصاح عن أي عمل أو مهمة كُلفوا بأدائها بصفتهم يحملون منصباً مستشاراً أو عاملاً مؤقتاً لدى Citi أو أي من شركاتهم السابقة (بما في ذلك، على سبيل المثال لا الحصر: Citibank و/أو Citicorp و/أو Travelers و/أو Salomon Brothers و/أو Smith Barney).

6-15 السجل التعليمي

يجب على المورد أن يتحقق من إتمام موظفيهم لأعلى مستويات التعليم. وينبغي أن تتضمن المعلومات التي يتم التحقق من صحتها تواريخ الالتحاق واسم (أسماء) المؤسسات التعليمية، والعنوان (العناوين) والدرجة (الدرجات) التي تم الحصول عليها.

7-15 الخلفية الجنائية

حيثما يكون مسموحًا بذلك قانونًا، يجب على أي موظف أو مقاول من الباطن تابع للمورد أن يفصح إلى Citi إذا ما تعرض للاعتقال أو الاستدعاء أو المثل 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، أو أي جرائم مماثلة التي تكون محددة بشكل مختلف بموجب القانون المحلي، باستثناء ما يكون 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.

8-15 إعادة الفحص

يجب إعادة فحص موظفي المورد الذين يتم إنهاء تكليفهم في حالة إعادة تكليفهم بمهام جديدة لدى Citi. وللاطلاع على مزيد من المعلومات حول متطلبات إعادة الفحص، يرجى الرجوع إلى https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

9-15 الانتقالات الدولية

يجب إتمام جميع عمليات الفحص وفقًا للوائح البلد الذي يكون فيه التكليف. وإذا انتقل أي من موظفي المورد إلى بلد جديد، فيجب إعادة فحص ذلك الفرد وفقًا لمتطلبات البلد الجديد.

16 النفقات

الموردون المؤهلون حسب التعاقدات للمطالبة بنفقات أعمال واجبة السداد.

1-16 نظرة عامة

لن يسدد Citi سوى النفقات المعقولة المتعلقة بالأعمال والتي اعتمدها مسبقًا بشكل كتابي وتكدها المورد فيما يتعلق بتقديم المنتجات والخدمات إلى Citi، ووفقًا لشروط العقد المعمول به أو سياسة حوكمة نفقات التشغيل المعمول بها لدى Citi، والمعايير والإجراءات ذات الصلة، حسب الاقتضاء، ويتم إثباتها بشكل كافٍ بالإيصالات الثبوتية أو الفواتير أو جداول رحلات السفر أو غيرها من أشكال الوثائق التي يعتبرها Citi مقبولة.

2-16 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 المورد نيابة عن المورد. ويجب أن تتضمن أي نفقات تُرسل إلى Citi بشأن سداد أي من عناصر النفقات الصالحة والمعتمدة (إضافة إلى جميع متطلبات الفترة الأخرى) ما يلي:

- 1- الغرض التجاري من النفقات؛
- 2- قيمة النفقات ووصفها؛
- 3- مكان وتاريخ النفقات؛

- 4- اسم/وصف المشروع الذي يقدم المورد الخدمات فيما يتعلق به؛
- 5- أسماء وعلاقة العمل الخاصة بممثل Citi الذي طلب الحصول على الخدمة (الخدمات) التي نشأت النفقات بشأنها؛
- 6- رقم أمر الشراء، عند الاقتضاء.

للاطلاع على معلومات بشأن النفقات التجارية القابلة للسداد والمسموح بها، يرجى التواصل مع جهة الاتصال الرئيسية للأعمال في Citi. يجب إرسال الإيصالات أو الفواتير أو جداول رحلات السفر أو غيرها من أشكال الوثائق الداعمة التي يعتبرها Citi مقبولة مع مطالبة السداد. يجب أن تكون مطالبات السداد متوافقة مع الأحكام الواردة في العقد المعمول به أو مع سياسة حوكمة نفقات التشغيل الخاصة المعمول بها لدى Citi والمعايير والإجراءات ذات الصلة، حسب الاقتضاء، ويجب كذلك اعتمادها من جانب شركة راعية مناسبة و/أو جهة الاتصال الرئيسية للأعمال في Citi، ويجب اعتمادها من جانب فرد تم تفويضه أصولاً ولديه مبلغ كافٍ للسلعة المقابلة. ولن يتم سداد الطلبات غير المستوفية للمتطلبات.

17 أمان المعلومات (IS)

يسري على الموردين بمن في ذلك المقاولين من الباطن الذين يمكنهم الوصول إلى/معالجة/تخزين/إدارة أي معلومات تخص Citi حسبما هي مصنفة ومحددة في الملحق؛ أو استضافة تطبيقات الإنترنت التي تحمل علامة Citi التجارية؛ أو الذين لديهم اتصال بموارد شبكة Citi، أو الذين يحتاجون إلى وصول دون مرافقة إلى مرافق Citi.

1-17 نظرة عامة

يوفر هذا القسم الحد الأدنى من المتطلبات الخاصة بمورد Citi، بمن في ذلك معالجي البيانات الفرعيين أو المقاولين من الباطن التابعين للمورد، الذين يقومون بتخزين معلومات Citi أو معالجتها أو إدارتها أو الوصول إليها أو استضافة تطبيقات Citi أو الذين لديهم اتصال بالشبكة مع Citi، فيما يتعلق بضوابط حماية المعلومات التي يتوقعها Citi. تضمن هذه المتطلبات حماية المعلومات وفقاً للمتطلبات القانونية والتنظيمية المعمول بها وأعلى معايير الصناعة (مثل ISO / IEC 27001/2) في المواقع التي يزاول فيها Citi ومورده 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 الموردين الامتثال لهذه القوانين أو اللوائح أو المعايير. وإضافة إلى ذلك، قد يُطلب من الموردين تضمين ممارسات وإجراءات إضافية فيما يتعلق بأمان المعلومات كجزء من امتثالهم لسياسات Citi والشروط والأحكام التعاقدية. إذا قرر أي من الموردين تنفيذ ممارسات أو إجراءات أمنية إضافية فيما يتعلق بأمان المعلومات، يجب على المورد التأكد من أن هذه الممارسات والإجراءات لا تتعارض مع الحد الأدنى من الضوابط المحددة في هذا القسم.

2-17 حوكمة وسياسة أمن المعلومات

يجب أن يكون لدى الموردين سياسات ومعايير موثقة خاصة بأمان المعلومات. يجب أن تتضمن حوكمة السياسة أدواتاً ومسؤوليات محددة بوضوح، ومراجعة/تحديث سنوي للسياسة والمعايير، لتكون متوافقة مع حالة التكنولوجيا الحالية، ومعايير الصناعة، والمتطلبات القانونية والتنظيمية.

3-17 فصل المهام

يجب أن يكون لدى الموردين إجراءات مطابقة لضمان عدم تمكن أي فرد من أداء أي وظيفتين تجاريتين أو وظيفتين من وظائف تكنولوجيا المعلومات (IT)، أو وظيفتين من وظائف أنظمة المعلومات الخاضعة للرقابة، مع وجود وصول مستمر لنفس النشاط أو التغيير أو نظام المعلومات أو المعاملة دون الحصول على إذن أو دون أن يتم الكشف عن ذلك، ما لم تكن هناك ضوابط تعويضية كافية للتخفيف من المخاطر.

الجدول (أ)

الوظائف	وصف الوظيفة
التطوير/الهندسة	تصميم أو إنشاء أو تعديل البرامج والأجهزة والتكوينات؛ وقد تشمل الأمثلة على ذلك: - تصميم وإنشاء كود تطبيق جديد ومخططات قواعد البيانات ذات الصلة

- هندسة منتجات البنية التحتية ومكونات التطبيقات - تخصيص منتجات التكنولوجيا لدمجها مع البرامج والخدمات	
الموافقة على ترقية التغييرات البرمجية المقرر تنفيذها	الاعتماد
تثبيت أو نشر أو إدارة التغييرات في البرامج والأجهزة والتكوين. وقد تشمل الأمثلة على ذلك ما يلي: - تنفيذ إصدار التعليمات البرمجية آلياً أو يدوياً إلى البنية التحتية للإنتاج - تثبيت منتج أو جهاز تكنولوجي - بدء أو إيقاف الخدمات لدعم استكشاف الأخطاء وإصلاحها في الأنظمة التي تحتوي على بيانات إنتاجية	تنفيذ/إدارة الأنظمة
التحقق من نشاط إدارة التغيير أو أحداث النظام المتعلقة بالأمان (مثل الاحتفاظ بسجلات التدقيق)	مراجعة نشاط معرف الهوية (ID) المتميز
إضافة وتعديل وحذف IDs (المستخدم، FIDs، والبوتات) أو الصلاحيات أو كلمات المرور	إدارة معرف الهوية (IDs)
وصف الوظيفة	وظائف الأعمال
بدء (يشار إليه أيضاً بإدخال أو إجراء أو إنشاء) معاملات تجارية وتغيير معلومات العميل	بدء معاملة تجارية
الموافقة على المعاملات التجارية (يشار إليها أيضاً بالتصريح بتلك المعاملات أو التحقق منها أو إصدارها)	اعتماد معاملة تجارية
وصف الوظيفة	وظائف IT
إدارة الأجهزة والدعم التشغيلي للمنتجات التي توفر خدمات البنية التحتية للشبكة. ومن الأمثلة على ذلك أجهزة توجيه الشبكة والمحولات وجدران الحماية وخدمات أسماء النطاقات (DNS)	عمليات الشبكة
إدارة الأجهزة والدعم التشغيلي للمنتجات التي لا توفر خدمات البنية التحتية للشبكة. ومن الأمثلة على ذلك الخوادم والهواتف وأجهزة الكمبيوتر	العمليات غير التابعة للشبكة

4-17 التزام الإدارة بأمن المعلومات

يخضع الموردون، الذين سيستضيفون أحد تطبيقات واجهة الإنترنت التي تحمل علامة Citi التجارية و/أو الذين تم السماح لهم بالوصول إلى معلومات Citi المصنفة باعتبارها سرية أو عليا، لعملية تقييم لأمن المعلومات من طرف خارجي (TPISA) لصالح Citi لتقييم سياسات الموردين وإجراءاتهم وضوابطهم فيما يتعلق بالامتثال لمتطلبات Citi وأي متطلبات قانونية و/أو تنظيمية (منطقة على Citi أو على المورد) تتعلق بأمان المعلومات.

وسوف يتألف التقييم من استبيانات أمنية تتطلب إجابات من المورد مع أدلة ثبوتية، وقد تتضمن زيارات إلى مواقع المورد حيث يتم تخزين المعلومات السرية أو العليا لدى Citi أو معالجتها أو إدارتها أو الوصول إليها بواسطة طرف ثالث. بالإضافة إلى ذلك، يجوز أن يقوم فريق المراقبة المستمرة التابع لجهة خارجية المعني بتقييم TPISA بمراقبة المورد باستخدام أدوات مراقبة الأمن السيبراني التي تستفيد من المعلومات المتاحة للجمهور لتحديد الأنظمة والمضيفين والتطبيقات والخوادم المعرضة للخطر على الإنترنت فيما يتصل بتلك الأشياء من قبيل البرامج التي انتهت صلاحيتها أو المنافذ المفتوحة المستغلة أو الثغرات الأمنية أو غيرها من الاختراقات. وإذا ما كشفت النتائج التي توصل إليها تقييم TPISA إلى وجود مواطن قصور أمنية أو أشارت إلى تلك المواطن، فسيقوم Citi بتوثيق النتائج في إخطار يتم تقديمه إلى المورد كما سيعمل مع المورد لتحديد الوسائل اللازمة لتصحيح مواطن القصور هذه. يجب على الموردين على وجه السرعة إجراء التصحيحات و/أو ضوابط التعويض الضرورية لمعالجة مخاوف Citi وفقاً لتقدير Citi وحده، وتلبية الأطر الزمنية المطلوبة وهي 180 يوماً تقويمياً بالنسبة للمشاكل عالية المخاطر، و 240 يوماً تقويمياً بالنسبة للمشاكل متوسطة المخاطر، وقبل تاريخ الامتثال التالي بالنسبة للمشاكل منخفضة المخاطر، حيث يتم تصنيف تلك المشاكل حسب المخاطر من قبل Citi.

1- يجب على المورد إجراء تقييمات منتظمة لعملياته التجارية والضوابط ذات الصلة وفقاً لمعايير وسياسات وإجراءات أمان المعلومات المطبقة لديه. يجب أن تتضمن التقييمات الدورية، كحد أدنى، ما يلي:

(أ) تقييم العمليات التي يستخدمها المورد لضمان الامتثال لسياسة ومعايير أمان المعلومات الخاصة بالمورد؛

(ب) تقييم الموارد الداعمة، مثل التطبيقات والبنية الأساسية المستخدمة بواسطة المورد وعمليات أمان المعلومات التي يستخدمها المقاولون من الباطن التابعين للمورد (عند الاقتضاء) والتي تدعم عملياتهم التجارية، أو تتيح إلى Citi إجراء هذه التقييمات. ويكون الامتثال لازماً في حال توقيع طرف ثالث على عقد جديد أو تجديده لعقد حالي مع مقاول من الباطن يمكنه الوصول إلى معلومات Citi المُصنّفة من جانب Citi باعتبارها سرية أو عليا أو معالجتها أو إدارتها أو التخلص منها.

2- يجب توثيق المشاكل التي تم تحديدها نتيجة لأي تقييم لمخاطر أمان المعلومات (مثل TPISA) وتتبعها حتى الإغلاق مع تقديم الأدلة على حل تلك المشكلات إلى Citi.

3- إذا تم نقل وظيفة إدارة أمان المعلومات الخاصة بالمورد عبر حدود الدولة، فيجب على المورد الحصول على موافقة موثقة من Citi قبل إعادة النقل هذه.

4- إذا استحوذ المورد على كيان جديد، فيجب على المورد إتمام تقييم الكيان المستحوذ عليه للامتثال لهذه المعايير.

5- يجب على المورد 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 يوافق Citi كتابةً على هذا التعهيد مُقدماً.

6- إذا استضاف المورد برنامج أو موقع إلكتروني يحتوي على معلومات Citi أو موسوم بعلامة Citi التجارية، فيجب إجراء تقييمات دورية للثغرات الأمنية وفقاً إلى System Security Testing Standard (SSTS) لدى Citi ويجب معالجة أي مشكلات جوهرية يتم تحديدها أثناء التقييم ضمن الأطر الزمنية المحددة في ذلك المعيار. حيث أن معيار SSTS غير معتمد للتوزيع الخارجي، فيجب على الموردين العمل مع مدير علاقات Citi الخاص بهم لضمان الامتثال للوثائق المرجعية. بالإضافة إلى ذلك، يجب على المورد الامتثال لمعايير إدارة أمان المعلومات ISO/IEC 27001 ذات الصلة (أو معايير إدارة أمان المعلومات اللاحقة التي تضع معايير وبروتوكولات أعلى)، كما يجب عليه الالتزام بأحكام أمان المعلومات التي يتضمنها هذا القسم رقم (17).

7- إذا دعت الحاجة إلى الاتصال بالخوادم و/أو نظم المعلومات على الشبكة الداخلية لدى Citi، يجب على المورد عندئذ إخطار جهة الاتصال الرئيسية للأعمال في Citi بحيث يمكن اتباع عملية توفير الاتصال الحالية.

8- يجب أن يخطر المورد بشكل فوري جهة الاتصال المناسبة لدى Citi (مسؤول نشاط الأعمال (BAO)) 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 أو معالجتها أو نقلها.

9- يجب على المورد التأكد من أن جميع الأنشطة عالية المخاطر أو التغييرات في البيانات الحساسة لها مسارات تدقيق توفر إمكانية نسب هذه الإجراءات إلى الأفراد الذين قاموا بها.

10- يجب على المورد ضمان إخفاء البيانات السرية أو العليا على الشاشات وفي الأوراق، ويشمل ذلك على سبيل المثال، تقارير الرصد والتجاوزات والتقارير التنظيمية وغيرها من التقارير).

11- يجب على المورد تقييم طباعة البيانات الحساسة أو تسجيلها أو نسخها، بما في ذلك ما يكون باستخدام "الأجهزة الخاصة" بالمورد نفسه. يجب على المورد إرجاع أو إتلاف جميع معلومات Citi في وقت زمني متفق عليه خلال الاتفاقية أو عند انتهائها، ما لم يكن ذلك محظوراً وفقاً للقانون أو اللوائح بأي شكل آخر.

- 12-** يجب على المورد أن يتأكد من توقيع جميع العاملين لدى المورد (الموظفين، المقاولين، الموظفين المؤقتين، المقاولين من الباطن) ممن يمكنهم الوصول إلى معلومات Citi على اتفاقية عدم الإفصاح أو اتفاقية السرية.
- 13-** يجب تزويد موظفي المورد بدليل الموظف أو وثيقة مماثلة تنطوي على إجراءات التأديب في حال انتهاك أو عدم الامتثال لمدونة قواعد السلوك لدى المورد وسياسات الموارد البشرية التي يجب الإقرار بها باعتبارها جزءاً من عملية التوظيف.
- 14-** يجب أن يكون لدى المورد إجراءات قائمة واجب اتباعها لاسترداد كل الأصول عندما يتم إنهاء عمل أي شخص سواء كان موظفاً أو غير موظف أو عند استقالته.
- 15-** في حالة الاحتفاظ بأي معلومات سرية، أو تخزينها بأي طريقة على موقع ويب أو نظام يمكن الوصول إليه عبر الويب، يجب على المورد الإفصاح إلى Citi عن تلك المعلومات؛ ويجوز إدراج هذا الإفصاح في وصف الخدمات. في حالة احتفاظ المورد بمعلومات Citi السرية أو تخزينها، يلتزم المورد بإجراء تدقيق (SSAE 18) (أو أي تقييم رسمي لاحق معتمد من جانب Citi) مرة واحدة سنوياً خلال مدة هذه الاتفاقية، ويلتزم بأن يقدم إلى Citi، مرة واحدة سنوياً على الأقل، نسخة من التقارير التي توثق نتائج ذلك التدقيق (SSAE 18) أو أي تقييم رسمي لاحق معتمد من جانب Citi.
- 16-** في حالة الاستحواذ على المورد - أو استحواذ المورد على كيان آخر، في أي عملية اندماج أو استحواذ أو معاملة مماثلة، مع احتمالية تأثير هذه المعاملة على الخدمات، يجب على المورد إخطار Citi كتابياً على الفور ويجب على المورد إجراء تقييم لأمان المعلومات على الكيان الناتج بما يتفق مع هذه المتطلبات من أجل التأكد من أن هذا الدمج أو الاستحواذ لا يؤثر على الامتثال لهذه المتطلبات.

5-17 مخاطر أمان المعلومات فيما يتصل بالمقاولين من الباطن

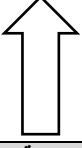
يجب على المورد أن يلزم المقاولين من الباطن الذين يمكنهم الوصول إلى بيانات Citi السرية أو العليا الخضوع لتقييمات أمن المعلومات (IS) قبل إبرام العقد وبعده بشكل دوري ويقوم بها موظفو أمان المعلومات المؤهلون. ينبغي أن تتم هذه التقييمات وفقاً لعملية معتمدة من الإدارة تتناول جميع مراحل عملية التقييم من البداية وصولاً إلى إدارة المشكلة. يجب أن يعتمد تقييم أمن المعلومات (IS) بخصوص المقاول من الباطن على أداة استبيان أو أداة مكافئة لتقييم وضع المقاول من الباطن ضمن نطاقات أمن المعلومات (IS) التي تتوافق مع تلك المتضمنة في استبيان Citi لتقييم أمن المعلومات للأطراف الثالثة (TPAQ) ويجب أن يتضمن طريقة منطقية لحساب مخاطر أمن المعلومات (IS) المرتبطة بمشاركة المقاول من الباطن. يجب على المورد تتبع إتمام التقييم وإدارة المشكلات المسجلة وخطط الإجراءات التصحيحية حتى إغلاق تلك المشكلات.

6-17 المسؤولية عن الأصول

- 1- يجب على المورد التأكد من الاحتفاظ بجرد لجميع التطبيقات والأجهزة الخاضعة لسيطرته والتي تستخدم لتخزين معلومات Citi و/أو معالجتها و/أو نقلها.
- 2- يجب على المورد التأكد من الاحتفاظ بجرد أصول Citi المعلوماتية تحت سيطرته وفقاً لإجراءات تُستخدم لضمان دقة واكتمال الجرد بشكل مناسب.
- 3- يجب أن يكون المورد مسؤولاً عن حماية جميع معلومات Citi التي تقع تحت سيطرته.
- 4- يجب على المورد ضمان المسؤولية عن نشاط المستخدمين بطريقة تتفق مع ممارسات الصناعة.
- 5- يجب تقييد وصول المستخدم إلى حسابات تخزين البريد الإلكتروني الخارجية الشخصية على الإنترنت وحسابات التخزين السحابي من الشبكة العالمية للمورد والتي توجد عليها معلومات Citi.

7-17 تصنيف المعلومات والتعامل معها.

يصنف Citi المعلومات وفقاً لجدول تصنيف المعلومات أدناه. يُرجى الاطلاع على الملحق للحصول على تعريفات وأمثلة على كل تصنيف معلوماتي مدرج أدناه.

مقيدة	أكثر حساسية
PII حساسة	
PII سرية	
سرية	
PII داخلية	
داخلية	
عامة	أقل حساسية

- 1- بناءً على تصنيف معلومات Citi، يجب على Citi أن يعمل مع المورد على تحديد المستوى الأمني المطلوب لحماية هذه المعلومات ويجب على المورد ضمان وجود ضوابط كافية، إلى جانب جميع المستويات المشددة أو المعدلة التي قد يطلبها Citi.
- 2- يجب تخزين المعلومات الداخلية أو العليا على الأجهزة التي يديرها طرف ثالث وفقاً لعقد مبرم بين الطرف الثالث و Citi يحتوي على أحكام تختص بالسرية بما يتوافق مع سياسات ومعايير Citi.
- 3- إذا سمح المورد باستخدام أجهزة غير أجهزة الشركة لتخزين بيانات Citi (أي الأجهزة التي تديرها أطراف رابعة)، فيجب عليه وضع سياسة تتطلب أن تخضع لموافقة إدارة معينة ووضع إرشادات معمول بها وإجراءات مراقبة حول كيفية استخدام معلومات Citi والتصرف فيها.
- 4- يجب على المورد دائماً حماية معلومات Citi من الوصول أو التعديل أو الحذف غير المصرح به.
- 5- معلومات Citi المُصنّفة باعتبارها سرية أو علنياً ويتم نقلها عبر وسائط قابلة للنقل إلكترونياً (ETM) يجب أن تكون مشفرة باستخدام خوارزمية ويجب تأكيد الاستلام. يجب على المورد التأكد من استلام ETM من قبل المستلم المقصود. وفي حالة عدم تلقي الإيصال في تاريخ الاستلام المتوقع، يجب على المورد إخطار Citi.

8-17 التهينة الآمنة

- 1- يلتزم المورد بالحفاظ على معيار تهينة آمن موثق لكل الأصول مع احتمالية تخزين معلومات Citi أو معالجتها أو الوصول إليها أو نقلها.
- 2- يجب على المورد تضمين ضوابط أمن المعلومات في عملياته وإجراءاته من أجل اختيار التطبيقات والمنتجات والخدمات وتطويرها وتنفيذها.
- 3- يجب أن يكون لدى المورد إجراء بناء آمن لجميع الأنظمة التي يتم فيها تخزين معلومات Citi و/أو معالجتها و/أو نقلها.
- 4- يجب على المورد الاحتفاظ بصورة آمنة أو قالب آمن لكل الأنظمة.
- 5- يجب إزالة كل حسابات وكلمات مرور المستخدم الافتراضية و/أو تغييرها من الأنظمة المدعومة بواسطة الموردين وأجهزة الشبكات والتطبيقات.
- 6- أي نظام أو خدمة تم اختراقها يجب إعادة بناؤها وتهينتها باستخدام صورة أو قالب يستند إلى سلامة مؤكدة.
- 7- أي تغيير يُجرى على تهينة آمنة يجب اعتماده من جانب الإدارة عبر عملية إدارة التغييرات لدى المورد.
- 8- يجب على المورد إخطار Citi بأي تغييرات في التهينة الآمنة.
- 9- يجب أن يتضمن إجراء البناء الأمن أدوات لدعم فحوصات إعدادات الأمان الآلية/معايير بناء الإعدادات في وقت نشر الإنتاج، والمراقبة المستمرة للتحقق من الامتثال للتهينة الأساسية والتحقق من أي انحرافات عنها.

9-17 متطلبات التشفير

يجب ألا يقوم المورد بإرسال معلومات مصنفة على أنها سرية أو علنياً بدون تشفير. يجب تشفير المعلومات المصنفة على أنها سرية أو علنياً **تشفيراً تاماً** باستخدام أدوات أو حلول معتمدة من Citi. البروتوكولات المعتمدة وأرقام الإصدارات ذات الصلة بالنقل المشفر للبيانات هي كما يلي:

- 1- عند تبادل معلومات المصادقة والتفويض: SAML v2.0، و OAuth v2.0 (التفويض فقط)،
- 2- لحماية قنوات الاتصال وما يرتبط بها من تبادل المفاتيح، لا يُسمح إلا بروتوكولات أمان الشبكات التالية:
 - (أ) يُفضل استخدام TLS v1.3 ويسمح بجميع مجموعات TLS v1.3. إذا كان TLS v1.3 هو البروتوكول الوحيد المُفعّل، فلن تكون هناك حاجة إلى مراجعة إضافية.
 - (ب) في حالة عدم جدوى TLS v1.3 من الناحية التقنية واستخدام TLS 1.2، فإن الدرجة (B) أو

أعلى من SSL Labs تكون مقبولة حاليًا ولا يلزم إجراء مراجعة إضافية.

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

1- **Advanced Encryption Standard (AES):** أطوال المفاتيح المعتمدة: 256 بت أو أكثر.

الأوضاع المحظورة: يُحظر وضع الكود الإلكتروني (ECB) إلا إذا كان مقدار النص العادي أقل من أو يساوي طول الكتلة. تشفير محرك الأقراص: يلزم استخدام مقياس التشفير المتقدم AES بمفتاح 256 بت. يُسمح بمقياس التشفير المتقدم AES بمفتاح بطول 128-bit كخيار TLS Cipher؛ ومع ذلك، سيتم رفض هذا لصالح 256-bit أو أعلى بحلول 31 ديسمبر 2028 لتمكين توافق Citi مع الجداول الزمنية الدولية (المرجع NIST 8547 IPD).

2- **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.

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

الإشعار المتعلق بالجاهزية الكمية للمورد: يجب على الموردين تقديم خطتهم بشأن تغطية الجدول 2 والجدول 4 من NIST IR 8547 (ipd) إلى فريق برنامج Citi Quantum Readiness عبر [\(survey link\)](#).

1- أنظمة تشفير المفتاح العام والحد الأدنى لأحجام طول المفتاح:

- (أ) Rivest–Shamir–Adleman (RSA): 2048 بت.
- (ب) Digital Signature Algorithm (DSA): 2048 بت. يجب عدم استخدام خوارزمية التوقيع الرقمي DSA لتأمين بيانات Citi التي تتم معالجتها أو تخزينها خارج Citi.
- (ج) Elliptic Curve Digital Signature Algorithm (ECDSA): 256 بت وكما هو محدد في ANSI X9.62 مع المنحنيات الموصى بها من قبل NIST.

2- آليات تبادل المفاتيح والاتفاقية والحد الأدنى من أحجام طول المفتاح:

- (أ) Diffie–Hellman (DH) / Ephemeral Diffie–Helman (DHE): 2048 بت.
- (ب) Elliptic-curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE): 256 بت وكما هو محدد في ANSI X9.63 مع المنحنيات الموصى بها من قبل NIST¹.

3- وظائف ملخص الرسالة: يُحظر إنشاء مفتاح تشفير بطول أكبر من عدد البتات العشوائية في المادة المستخدمة لإنشاء التجزئة.

- (أ) SHA-1 مقبول فقط لتطبيقات التوقيع غير الرقمي. مجموعة SHA-2 ومجموعة SHA-3 و POLY-1305: مقبول لجميع تطبيقات دالة التجزئة المشفرة.

4- وظائف اشتقاق المفاتيح المعتمدة على كلمة المرور والحد الأدنى من المتطلبات:

- (أ) PBKDF2: الحد الأدنى لعدد التكرار 10000 مع قيمة مضافة للحماية لا يقل عن 16 بايت.
- (ب) HKDF: يجب أن تكون هذه الوظيفة مصحوبة بقيمة مضافة للحماية، ويجب تضمين قيمة إدخال المعلومات.
- (ج) SCRYPT: الحد الأدنى لعدد الجولات/عامل التكلفة هو 10.
- (د) يحظر استخدام NIST SP800-108 KDF لتشفير البث. يُسمح باستخدام أوضاع NIST SP 800-108 KDF، وهي أوضاع العداد والتغذية الراجعة وتكرار خط التدفق الأنوبي المزوج.
- (هـ) يُنصح باستخدام Argon2.

5- دوال التجزئة لكلمة المرور والحد الأدنى من المتطلبات:

- (أ) Bcrypt (للتخزين المحلي لمواد المصادقة): يجب ألا يقل الحد الأدنى لعدد الجولات/عامل التكلفة عن 10.

¹ يُفضل استخدام ECDHE.

ب) يوصى باستخدام Argon2 أو PBKDF2 لتجزئة كلمة المرور عند تخزين كلمات المرور محليًا على أي بيانات أو أنظمة يتم نشرها بواسطة المنتج الخاص بالمورد.

10-17 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 المورد. بروتوكولات البريد الإلكتروني الآمنة المعتمدة هي:

- 1- بروتوكول التشفير على أساس التعريف (IBE) يتميز ببريد إلكتروني مشفر ويمكن استخدامه ضمن الحلول التي تواجه عملاء Citi وأنظمة البريد الإلكتروني والتسليم الإلكتروني الآمنة فقط.
- 2- بروتوكول TLS الإلزامي (MTLS) يتميز بروتوكول MTLS بتشفير الجلسات (لا يشفر حمولة البريد الإلكتروني) ويمكن استخدامه مع البائعين والشركاء والعملاء الذين تفاوضوا مسبقًا على استخدامه.
- 3- بروتوكول البريد المعرف بمفاتيح المجال (DKIM) يتميز بمصادقة المصدر وإدارة المفاتيح ويمكن استخدامه مع البائعين والشركاء والعملاء.

11-17 الشبكات الخاصة

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

12-17 المكالمات الصوتية 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 المورد وضع إجراءات وتوجيهات محددة لحماية المعلومات السرية أو العليا التي يتم إرسالها من خلال تلك القنوات.

13-17 إدارة مفاتيح وشهادات التشفير

يشير مصطلح الحدود الآمنة المستخدم في هذا القسم إلى برنامج التحقق من صحة وحدة التشفير (CMVP)، مثل Federal Information Protection Standard (FIPS)، والحدود المحققة (FIPS 140-2/3) المستوى 2 هو الحد الأدنى المقبول لمستوى الأمان). (تكون معازل الحوسبة السرية مثل AWS Nitro Enclaves مقبولة. يجب أن تتم الموافقة على الحالات الأخرى الخاصة بالحدود الأمنية الفريدة من قبل Citi).

- 1- يجب على المورد نشر خوارزميات تشفير قياسية مُستخدمة في المجال والحد الأدنى من أطوال المفاتيح لأغراض التشفير والتوقيع (بما في ذلك مفاتيح SSH). يجب على المورد تقديم ضمانات من خلال عملية إدارة التغيير المتبعة لديه عند تحديث تلك الخوارزميات وأطوال المفاتيح لتتوافق مع معايير الصناعة.
- 2- يجب أن يكون لدى المورد عملية دورة حياة رسمية موثقة لإدارة المفاتيح والسرية والشهادات مع وجود ضوابط لحماية المواد الحساسة من الاستخدام أو التعرض غير المصرح به. يجب أن تتم جميع أحداث دورة حياة أسرار التشفير والمفاتيح داخل حدود آمنة فقط. يجب توثيق جميع عمليات الوصول إلى الحدود المميزة والأمنة. يجب على المورد توفير مخطط تسلسلي لجميع أحداث دورة حياة المفاتيح مع إبراز الأطراف الفاعلة والكيانات والحدود المعنية.
- 3- يجب أن يكون لمفاتيح التشفير غرض فريد ويجب ألا تستخدم أبدًا لأي غرض آخر، مثل استخدام نفس مفتاح التشفير لتشفير القرص وكذلك تشفير البيانات أو نفس مفتاح التشفير لتشفير الحمولة وكذلك تشفير قاعدة البيانات. يُحظر افتراضيًا على مورد البرمجيات كخدمة (SaaS) إعادة استخدام مفاتيح التشفير عبر مستأجرين متعددين، ولا يُسمح بذلك إلا في حالات الاستخدام غير الحرجة ومنخفضة المخاطر التي تتضمن معلومات Citi المصنفة ضمن فئات أقل من PII سرية و PII حساسة ومقيدة، وذلك رهنًا بموافقة صريحة من مجلس هندسة الأمن.
- 4- بالنسبة لجميع مفاتيح التشفير (المتماثلة أو غير المتماثلة)، يجب عدم عرض المفتاح الخاص أو مادة المفتاح الخاص (مثل المكونات الرئيسية أو جزء من مفتاح خاص) في هيئة نص واضح في أي وقت. يجب ألا يغادر

المفتاح الخاص أو مادة المفتاح الخاص (مثل المكونات الرئيسية أو جزء من مفتاح خاص) الحدود الأمانة باستثناء المفاتيح المؤقتة مثل مفاتيح الجلسة الديناميكية. إذا استلزم التصميم نقل مفتاح متمثل أو مفتاح خاص أو بيانات مفتاح خاص بين مناطق أمانة/حدود وصول مميزة، فيجب نقلها في شكل مشفر فقط باستخدام مفتاح Symmetric Key Wrapping Key أو مفتاح Public Key Transport Key عبر أنفاق TLS المشفرة المتبادلة فقط، ويجب الموافقة على ذلك النقل من قبل Citi كتابيًا. يجب ألا يغادر مفتاح النقل الخاص أبدًا حدود الوصول الآمن المتميزة التي تم إنشاؤه فيها في هذه الحالات.

5- يجب تقسيم مفتاح تشفير المفتاح المتمثل إلى مكونين رئيسيين أو أكثر وأن يتم تشفيره باستخدام XOR قبل التوزيع ولإدخال/تحميل المفتاح يدويًا. يجب أن يحتوي مفتاح Symmetric Key Wrapping Key على قوائم التحكم في الوصول (ACLs) ملائمة مرتبطة داخل الحدود الأمانة مثل الوحدات النمطية المصادق عليها بواسطة برنامج CMVP ويجب ألا يتم تخزين مفتاح Symmetric Key Wrapping Key خارج الحدود الأمانة.

6- يجب فصل وصول العامل البشري أو الخدمة أو الوكيل المؤتمت إلى مخازن المفاتيح أو الحدود الأمانة التي تتضمن مفاتيح أو أسرار خاصة أو مواد المفاتيح الخاصة (مثل المكونات الرئيسية أو جزء من مفتاح خاص) بشكل صحيح مع وجود عناصر تحكم تقصر الوصول فقط على الموظفين المصرح لهم أو الأنظمة المصرح لها.

7- يجب تسجيل كل طلب للوصول إلى مخازن المفاتيح التي تحتوي على مفاتيح خاصة أو متماثلة وتوثيقه بتفاصيل مثل من ومتى والغرض من الوصول لأغراض التدقيق.

8- يجب على المورد عدم استخدام الشهادات الموقعة ذاتيًا وشهادات أحرف البديل Wildcard أو شهادات SSL الافتراضية.

9- يجب أن يكون لجميع مفاتيح التشفير فترة زمنية محددة للتشفير كما هو مقترح في NIST SP800-57 الجزء 1، المراجعة 6 يجب تحديث المفاتيح أو تدويرها قبل انتهاء الصلاحية لاستيعاب فترات التغيير وتضارب الجداول الزمنية وتجميد النظام.

أ) أثناء استبدال شهادة منتهية الصلاحية، يُحظر إعادة استخدام زوج المفاتيح غير المتمثل القديم.

10- يجب التعامل مع المفاتيح المشفرة على أنها مخترقة بمجرد الاشتباه في اختراق سلامة المفتاح، أو الوسيط الذي يُخزن أو يُشارك فيه، أو سرية المفتاح المتمثل أو الخاص. يجب إزالة جميع المفاتيح المخترقة من الاستخدام التشغيلي، ويجب إلغاء جميع الشهادات المقابلة.

11- يجب تشفير الشبكات اللاسلكية باستخدام خوارزميات التشفير القياسية المستخدمة في الصناعة.

12- يجب على الموردين الذين يستخدمون أي شكل من أشكال آلية التشفير استخدام الأدوات والأساليب القياسية المستخدمة في المجال لإدارة المفاتيح. يجب فصل دور الإدارة الرئيسية عن الإدارة التشغيلية.

13- يجوز للموردين استخدام أنظمة KMS و PKI السحابية فقط في حال ضمان التوافق مع خدمات PKI و KMS التي توفرها خدمات أمن بيانات Citi، وعدم تفويض التحكم في التشفير خارج نطاق حوكمة التشفير لدى Citi.

14-17 مسؤولية التحكم في الوصول

لحماية جميع أنظمة المعلومات الخاضعة للرقابة المستخدمة لتخزين معلومات Citi السرية أو العليا من أي وصول غير مصرح به و/أو الوصول إليها و/أو إدارتها و/أو معالجتها و/أو نقلها، يقع على عاتق المورد مسؤولية تطبيق مبدأ الأقل امتيازًا، وذلك من خلال تحديد استحقاقات المستخدم بالحد الأدنى من مستوى الوصول المطلوب لكل مهمة وظيفية ومن خلال إدارة توفير الوصول المنطقي إلى جميع الأنظمة والتطبيقات. يجب أن تكون عناصر التحكم موثقة بالكامل وقابلة للتدقيق. يجب أن يتم توفير الوصول وإلغاء توفيره، بما في ذلك إعادة تعيين كلمة المرور وتفعيلها، عبر عملية آلية كلما أمكن ذلك، لضمان الحد من مخاطر الخطأ البشري المحتمل الناتج عن منح صلاحيات زائدة، وللتوافق مع معايير الصناعة.

- 1- المورد هو المسؤول عن حقوق الوصول الخاصة بكل المستخدمين في مؤسسته.
- 2- يجب على المورد تنفيذ ضوابط الوصول التي تضمن عدم منح المستخدمين سوى تلك الامتيازات والاستحقاقات الضرورية للغاية لأداء وظائفهم.
- 3- يجب على المورد تطبيق إجراءات تضمن إزالة جميع إمكانيات الدخول الافتراضية أو تعطيلها أو حمايتها لمنع استخدامها على نحو غير مصرح به.

15-17 إدارة وصول المستخدم

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

- 1- تحديد وجرد أنظمة المصادقة المعتمدة.
- 2- اشتراط حصول كل أنواع الوصول إلى بيانات Citi على موافقة من مدير أو من ينوب عنه ومن مالك النظام. يقع على عاتق المورد مسؤولية ضمان منح موظفيه ممن لديهم حق الوصول إلى بيانات Citi ذلك الوصول على أساس الحاجة إلى المعرفة.
- 3- اشتراط عدم جواز منح مزيج من المزايا/الوظائف لمستخدم واحد إذا كانت ستمثل تضارباً في المصالح أو انتهاكاً لقواعد المنشئ-الفاحص.
- 4- عملية مراقبة للإشراف على حقوق الوصول الممنوحة/المُلغاة لكل مستخدم على النظام وإدارتها.
- 5- يجب ألا تعتمد طلبات الوصول على نسخ/استنساخ صلاحيات مستخدم آخر؛ بل يجب أن تحدد الطلبات أدواراً/صلاحيات واضحة مع تبرير تجاري لمنع التوسع غير المبرر في الصلاحيات وتطبيق مبدأ أقل الصلاحيات.

تعريف المستخدم والمصادقة عليه

16-17

يجب أن تصدق جميع أنظمة المعلومات الخاضعة لسيطرة المورد على هوية المستخدمين أو الأنظمة التي تصل إلى هذه المنصات قبل بدء أي جلسة أو معاملة حيث يمكن الوصول إلى معلومات Citi.

- 1- يجب أن يكون المستخدمون معرفين أو محددين بشكل فريد للمنصات التكنولوجية بواسطة معرف المستخدم.
- 2- يجب المصادقة على المستخدمين في المنصة التكنولوجية باستخدام طريقة مصادقة معتمدة، ويجب على المورد التواصل مع جهة الاتصال الرئيسية للأعمال (BAO) الخاصة به من أجل التعرف على الطرق المعتمدة الحالية.
- 3- يجب أن يتم استخدام جميع استخدامات البنية التحتية المشتركة للمصادقة (مثل تسجيل الدخول الفردي وتسجيل الدخول المختصر وخدمات المصادقة الأخرى المشتركة) وفقاً لمتطلبات المصادقة لدى Citi؛ ويجب على المورد التواصل مع BAO للتعرف على الطرق المعتمدة الحالية.
- 4- يجب أن تكون بيانات التحقق من الهوية (IVD) التي تُستخدم لمصادقة مستخدم في نظام معلومات سواء خلال إرسالها أو عند تخزينها. راجع القسم 9-17 للتعرف على متطلبات التشفير.
- 5- يجب ربط كل حساب يستخدمه موظفو المورد للوصول إلى أنظمة Citi بمعرف فريد -معرف معين لدى Citi (مثل GEID)؛ ويحظر تحديد معرفات المستخدم العامة/المشتركة للمستخدمين البشريين لضمان إمكانية التتبع وإنفاذ SOD والجاهزية للتدقيق.

تحديد الوصول المميز، والوصول المؤقت المميز

17-17

يجب على المورد الاحتفاظ بقائمة لجميع الهويات وتحديد تلك التي تمتلك حق الوصول المميز أو التي تمتلك حق الوصول إلى المستودعات الإلكترونية (مجموعات البيانات أو قواعد البيانات التي تدعم تطبيقات الأعمال) التي تحتوي على معلومات مصنفة على أنها PII سرية أو عليا. يجب على المورد تنفيذ الضوابط التي توفر الحماية من الاستخدام غير المصرح به لهذه الهويات. إذا احتاج أحد العاملين إلى الوصول إلى هوية متميزة أو إلى المستودعات الإلكترونية المذكورة من قبل، يجب أن يتم منح الوصول من خلال عملية إدارة الوصول المؤقت التي:

- 1- تقتضي أن يكون مقدم الطلب إما على قائمة المستخدمين المعتمدين مسبقاً أو يجب عليه الحصول على موافقة في وقت الاستخدام.
- 2- تتطلب تبريراً موثقاً في بطاقة التغيير/المشكلة قبل السماح بالوصول.
- 3- تتضمن مراجعة مستقلة للنشاط المنجز أثناء الوصول.
- 4- تتضمن عملية لبدء إلغاء/إزالة الوصول في نهاية مدة إصدار الوصول المؤقت.
- 5- 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.

مراجعة حقوق وصول المستخدم

18-17

- 1- يجب على المورد تطبيق عملية موثقة لمراجعة استحقاقات المستخدم في نظم المعلومات الخاضعة للسيطرة والمستخدم لتخزين معلومات Citi و/أو معالجتها و/أو إدارتها و/أو نقلها بصفة نصف سنوية على الأقل، والتحقق من هذه الاستحقاقات وإزالة غير الضروري منها.
- 2- يجب ألا يراجع المستخدمون أو يعتمدوا استحقاقاتهم أو استحقاقات الأفراد الذين أوكلوا إليهم مسؤولية المراجعة.
- 3- بعد أن يغير أي موظف لدى المورد أي وظيفة، تتاح للمورد 14 يومًا تقويميًا لمراجعة إمكانية الوصول والاستحقاق، وإزالة الوصول إلى بيانات Citi إذا لم يعد ذلك مطلوبًا للوظيفة الجديدة للموظف.

تأمين إجراءات تسجيل الدخول

19-17

- 1- 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.

نظام إدارة كلمات المرور

20-17

- 1- يجب ألا تُعرض كلمات المرور الثابتة للمستخدم على الشاشة بصيغة نصية واضحة. يُستثنى من هذا الشرط خاصية إظهار/إخفاء كلمة المرور، بشرط ما يلي:
 - (1) إخفاء إدخال كلمة المرور بشكل افتراضي،
 - (2) إمكانية إظهار كلمة المرور فقط من خلال إجراء صريح من المستخدم، (3) إعادة إخفاء كلمة المرور تلقائيًا في غضون 15 ثانية كحد أقصى بعد توقف المستخدم عن استخدام النظام.
- 2- يجب عدم إنشاء ترميز صعب لكلمات المرور الخاصة بالمعرف الوظيفي المميز بصيغة نصية واضحة.
- 3- يجب أن تحتوي كلمات المرور الثابتة على عشرة (10) رموز على الأقل، ويجب أن تحتوي على أحرف وأرقام، وتكون حساسة لحالة الأحرف. يجب التحقق من حساسية حالة كلمات المرور الثابتة في كل نقطة من نقاط المصادقة. يجب أن تحتوي كلمات المرور الخاصة بالمعرفات الوظيفية (FID) على 15 حرفًا على الأقل في التطبيقات التي تم نشرها بعد 31 أغسطس 2026.
- 4- 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).
- 5- يجب تغيير جميع كلمات المرور الثابتة كل 90 يومًا تقويميًا على الأقل.
- 6- يجب حظر جميع كلمات المرور الثابتة بعد ما لا يزيد عن ست (6) محاولات فاشلة متتالية لتسجيل الدخول، أو بعد ست (6) محاولات متتالية لإعادة تعيين كلمة المرور. يجب إلغاء تأمين كلمات المرور من خلال وظيفة مسؤول الهويات (ID)، أو إلغاء تأمينها تلقائيًا بعد 30 دقيقة على الأقل.
- 7- يجب على جميع أنظمة المصادقة فرض رقابة لعدم نشاط تسجيل الدخول/عدم الاستخدام بحيث لا يمكن أن تتجاوز 100 يوم تقويمي. وإذا كان ممكنًا من الناحية الفنية، يمكن أن يقوم المستخدم أو أي وظيفة أخرى مُصرح لها بإعادة تمكين تسجيلات الدخول المعطلة.
- 8- يجب أن تضمن عملية المصادقة عدم استخدام كلمة المرور نفسها ضمن التغييرات الستة (6) الأخيرة على الأقل.

استخدام الأدوات المساعدة للنظام

21-17

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

انقضاء مدة الجلسة

22-17

- 1- يجب أن يتم تسجيل الدخول أو إعادة المصادقة لجميع مستخدمي نظام المعلومات الخاضع لمراقبة المستخدم لتخزين معلومات Citi و/أو معالجتها و/أو نقلها.

2- يجب أن يُطلب من المستخدمين إعادة المصادقة بعد فترة من عدم النشاط لا تتجاوز 30 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.

23-17 إنهاء وصول المستخدم

- 1- بمجرد إنهاء عمل المستخدم أو استقالته، يجب أن يتم على الفور إزالة وصول المستخدم أو استحقاقاته التي تسمح بوصوله إلى بيانات Citi السرية أو العليا بما في ذلك تسجيل دخول المستخدم إلى سطح المكتب/الدليل النشط، وتسجيل الدخول الأحادي (SSO)، والبريد الإلكتروني، وكلمة المرور التي تُستخدم لمرة واحدة (OTP)، والرموز المميزة، والوصول عن بعد.
- 2- إذا كان للموظف حق الوصول إلى الأنظمة التي يملكها أو يديرها Citi، فيتم إخطار مدير علاقات أعمال Citi أو BAO أو دعم BAO فوراً بمجرد تغيير الوظيفة أو إنهاء عمل ذلك الموظف، لضمان قيام مدير علاقات أعمال Citi بإزالة الوصول للعاملين الذين تم إنهاء خدمتهم بحلول نهاية تاريخ إنهاء خدمتهم.
- 3- يجب أن يكون لدى المورد عملية موثقة واجب اتباعها لاسترداد إمكانية الوصول من جميع الأصول بما يتماشى مع الأطر الزمنية المنصوص عليها في القسم 2-23-17 عند إنهاء خدمة أحد الموظفين أو غير الموظفين أو استقالته.
- 4- في حالة اكتشاف أي خلل من قبل المورد فيما يتعلق بالأقسام 1-23-17 - 3-23-17، يجب على المورد إبلاغ مدير علاقات أعمال Citi أو BAO أو دعم مكتب BAO على الفور، مع تقديم مبررات وضوابط سليمة.

24-17 الوصول عن بُعد

يجب أن يكون لدى المورد ضوابط نافذة للوصول عن بُعد من أجل حماية الوصول إلى الشبكات التي من شأنها أن تخزن أو تعالج أو تنقل بيانات Citi السرية أو العليا ومن بينها:

- 1- 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.
- 2- جميع أجهزة الحاسوب المحمولة التي يديرها المورد وجميع أجهزة سطح المكتب التي يديرها المورد والمستخدم لتخزين معلومات Citi و/أو معالجتها و/أو نقلها، باستخدام الوصول عن بُعد حيث يوجد تخزين/معالجة محلية للمعلومات المصنفة في تصنيف معلومات Citi باعتبارها سرية أو عليا، يجب تشفيرها باستخدام أداة التشفير التي تلبي معايير الصناعة.
- 3- يجب أن يتم إنشاء الاتصالات عن بُعد من خلال حلول معتمدة للوصول عن بُعد والتي تستخدم مصادقة متعددة العوامل (MFA).
- 4- يجب أن تحتوي الأجهزة التي يديرها المورد على جدار حماية شخصي يتم تنشيطه عند توصيله مباشرة (أي ليس من خلال جدار حماية أو بروكسي يديره المورد) بالإنترنت.
- 5- يجب توصيل الأجهزة التي يديرها المورد بانتظام بشبكة المورد لتلقي وتثبيت التحديثات المنتظمة للبرامج/أدوات مكافحة الفيروسات كشرط أساسي للوصول الكامل إلى الشبكة. يجوز السماح بالوصول المحدود من أجل الغرض الصريح المتمثل في تحديث الجهاز.
- 6- إذا كانت الأجهزة التي لا يملكها ولا يديرها المورد تُستخدم للوصول إلى معلومات Citi السرية أو العليا، فيجب تهيئتها حتى تستخدم حلاً معتمداً لا يسمح بالتنزيل على الجهاز المحلي. يجب تنفيذ الضوابط التالية:
(أ) يُحظر تنزيل بيانات Citi على جهاز خارج نطاق حل تديره مؤسسة.
(ب) يجب على المورد التأكد من أن ذلك الوصول مؤمن سواء عن طريق المصادقة القائمة على الرمز أو القائمة على الشهادة باستخدام تقنيات الوصول عن بُعد القياسية (مثل واجهة سطح المكتب الافتراضية (VDI)).
(ج) يجب تكوين حلول الوصول عن بُعد مثل Terminal Services و VMWare Horizon لتعطيل مشاركة الحافظة وتعيين محرك الأقراص Drive Mapping عبر بروتوكولي Blast و PCoIP، وتعطيل بروتوكولات RDP و SSH.
- 7- في حالة استخدام رموز البرامج المميزة للمصادقة متعددة العوامل MFA، مثل الوصول إلى تطبيق برمجي على جهاز محمول، يجب أن يصادق برنامج مصادقة الرمز الرقمي على المستخدم (على سبيل المثال، عن طريق كلمة المرور، وما إلى ذلك)، ويمنع استخدامه إذا كان الهاتف المحمول مكسور الحماية أو متجذراً (باستخدام نظام تشغيل غير تلك المعتمدة والموفرة من قبل بائع الجهاز المحمول).

- 8- يجب أن تتم المصادقة فقط عن طريق المصادقة متعددة العوامل حيال جميع موظفي المورد 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 المورد من أجل الوقوف على أي نشاط مشبوه و/أو وصول غير مصرح به وفقًا لهذه المتطلبات.
- 9- بالنسبة للأجهزة المملوكة شخصيًا والأجهزة المملوكة لطرف ثالث، يجب أن يتوفر لدى المورد حل فعال لضمان أن تكون هذه الأجهزة مزودة بإصدار معتمد من نظام التشغيل، ومستويات التصحيح، وبرامج مكافحة الفيروسات، وحلول مكافحة البرامج الضارة، قبل السماح لهذه الأجهزة بالاتصال بالشبكة.
- 10- يجب على المورد ضمان تلبية جميع موظفيه لما يلي:
- (أ) الاحتفاظ بمساحة عمل خاصة ومخصصة عن بُعد لا تحتوي على أي أجهزة مساعدة صوتية (مثل Siri و 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.
- (ب) إغلاق الجهاز الحاسوبي عند ترك الجهاز دون مراقبة للتأكد من تخفيف الوصول غير المصرح به لعرض الشاشة بشكل مناسب.

25-17 سياسة المكتب النظيف

يجب على موظفي المورد حماية معلومات Citi بجميع أشكالها، بما في ذلك المعلومات المادية المستخدمة أو المخزنة في مكان عملهم. يتعين على الموردين إبلاغ هذا المطلب لكل الموظفين بصفة سنوية على الأقل من خلال تدريب نظم المعلومات (IS) أو أي قناة أخرى.

26-17 السلامة من الحرائق

- 1- يجب أن يمثل المورد للمتطلبات القانونية والتنظيمية السارية التي تحكم الأمان المادي وخلق بيئة عمل آمنة، بما في ذلك قوانين الحريق المحلية.
- 2- يجب على المورد استخدام نظام (أنظمة) للكشف عن الحرائق والإنذار بها وإخمادها. يجب فحص النظام (الأنظمة) بصفة نصف سنوية واختباره سنويًا.

27-17 الأمان المادي

- 1- يجب تخزين معلومات Citi في مناطق آمنة تتمتع بضوابط تقصر الوصول على الأفراد المصرح لهم فقط.
- 2- يجب أن يكون لدى المورد نظام تحكم في الوصول مادي موثوق وقابل للتدقيق.
- 3- يجب على المورد استخدام مزيج من أنظمة الإنذار/كشف التسلسل الأمنية التي تحتوي على إنذار أمني يراقبه طرف ثالث، وحراس الأمن والمراقبة عبر الفيديو حسب ما هو ملائم للبيئة والخدمات المقدمة.
- 4- يجب أن يكون لدى المورد سياسة موثقة للزيارات تحتوي على شرط يلزم جميع الزوار بتقديم هوية يمكن التحقق منها عند الوصول وتسجيل الدخول وتسجيل الخروج.

28-17 إجراءات ومسؤوليات أمان عمليات التشغيل

- 1- يجب أن تشمل عملية إدارة التغيير المتبعة لدى المورد على ضوابط رئيسية لنقاط التحقق الرئيسية حول تسجيل التغيير ومراجعته واختباره واعتماده وتنفيذه وإغلاقه. كما يجب أن يكون لدى المورد عملية تختص بالتغييرات الطارئة تتطلب جميع المراحل المذكورة بما في ذلك التسلسل الهرمي للموافقات الإلزامية.
- 2- يجب أن يكون لدى المورد عملية قابلة للتدقيق حول إدارة القدرات تتضمن (على سبيل المثال لا الحصر) مقاييس/مؤشرات التوافر والقدرة والأداء؛ وتقييم أثر الأعمال؛ والتتبع الاستباقي، والتحقيق في المشكلات الخاصة بالأداء والقدرة ومعالجتها.
- 3- يجب على المورد، حيثما أمكن، التأكد من أن جميع بيانات المختبرات والتطوير والاختبار والإنتاج منفصلة ماديًا و/أو منطقيًا عن بعضها البعض.

29-17 متطلبات تطوير البرمجيات

تتطبق على الموردّين الذين يقدمون البرامج التي تم تطويرها لاستخدام Citi الحصري. يجب على الموردّين الالتزام بهذه المتطلبات أو إثبات وجود عملية موثقة ومعتمدة تختص بدورة حياة تطوير البرمجيات ("SDLC") مع نهج مكافئ بنفس الجودة.

30-17 البدء والتخطيط

يجب على الموردّ تحديد نطاق الحل وأهدافه بما يتماشى مع متطلبات Citi والالتزامات التعاقدية. ويشمل ذلك ما يلي:

- 1- توثيق المتطلبات الوظيفية وغير الوظيفية؛
 - 2- تقديم تقديرات الجهد والإطار الزمني؛
 - 3- تحديد جميع مكونات أو تبعيات الطرف الثالث.
- يجب أن تبدأ أنشطة الامتثال، بما في ذلك تقييمات المخاطر الأمنية، مع بداية المشروع. يجب الإبلاغ بوضوح عن الأدوار والمسؤوليات ونقاط الفحص الخاصة بالموافقة.
- يجب تصنيف جميع البيانات على أنها بيئة تطوير (DEV) أو اختبار (TEST) أو إنتاج (PROD)، ويجب أن تظل منفصلة تمامًا طوال دورة الحياة. ويحدد تصنيف البيئة صلاحيات الوصول ونوع البيانات التي يمكن معالجتها. يجب على الموردّ تقييد الوصول بناءً على تصنيف البيئة ومواءمة عمليات النشر مع إكمال مرحلة SDLC المناسبة لمنع الوصول غير المصرح به أو تسريب البيانات.

31-17 التصميم

يجب على الموردّ توثيق نهج تصميم يضمن تلبية الحل الذي يتم تقديمه لجميع المتطلبات المذكورة (يُشار إليها باسم "خطة الاختبار"). يجب أن تتضمن خطة الاختبار وتصنف، كحد أدنى، ما يلي:

- 1- جميع الاختبارات التي سيجريها فريق التطوير، بما في ذلك اختبارات الوحدة والاختبارات الوظيفية وغير الوظيفية، واختبارات جوانب الأداء، مع إمكانية التتبع وصولاً إلى المتطلبات؛ و
 - 2- تحديد المُعتمد (المُعتمدين) الذي سيؤكد الإكمال؛ و
 - 3- متطلبات اختبار الأمان، مثل تقييمات الثغرات الأمنية ونمذجة التهديدات؛ و
 - 4- بيئة الاختبار والنهج والعملية ومسار الترقية.
- يجب إعداد استراتيجية إصدار تحدد الشروط المسبقة والعملية للإصدار في بيئتي TEST (الاختبار) و PROD (الإنتاج)، بما في ذلك معايير الجاهزية للإصدار، والمحتوى، وتواتر التسليم على مدار عمر المشروع. وحيثما ينص العقد على ذلك، يجب تجميع توزيعات البرمجيات بتنسيق معتمد من Citi باستخدام أدوات وإجراءات سير عمل معتمدة من Citi.

32-17 الاختبار

يجب تخطيط الاختبار وتنفيذه في بيئة خاضعة للرقابة للتحقق من تلبية الحل لمتطلبات محددة ومعايير نجاح محددة. يجب أن تكون حالات الاختبار قابلة للتتبع للتحقق من تلبية المتطلبات وتعديلات الكود.

يجب على الموردّ إعداد تقرير يلخص نتائج الاختبار/الإخفاق، والاختبارات الإضافية التي يتم إجراؤها أثناء التطوير، وأي اختبار لم يتم إكماله (مع ذكر الأسباب) (يُشار إليه باسم "تقرير الخروج من الاختبار"). ويجب توثيق العيوب والقدرات المؤجلة إلى جانب خطط التخفيف المتعلقة بالمسائل التي لم يتم حلها.

بناءً على طلب Citi، يجب على الموردّ تقديم أدلة على ما يلي:

- 1- خطة اختبار تفصيلية؛ و
- 2- إكمال الاختبار والنتائج التفصيلية في تقرير الخروج من الاختبار؛ و
- 3- إمكانية تتبع نتائج الاختبار للتحقق من تلبية المتطلبات وتعديلات الكود.

33-17 النشر

قبل النشر، يجب على الموردّ إكمال جميع الاختبارات الأمنية المطلوبة، بما في ذلك عمليات مسح الثغرات الأمنية ونمذجة التهديدات. ويجب أن تكون عملية الإصدار منظمة بحيث تتضمن سجلات التغييرات الموثقة، واستراتيجيات التراجع، والموافقات المطلوبة. يجب أن تتضمن خطط التنفيذ ودقات التشغيل الخاصة بالنشر بروتوكولات المراقبة والتصعيد.

بعد النشر، يجب على الموردّ وضع اللمسات الأخيرة على معرّفات النظام وتحديث جميع الأدوات الاصطناعية ذات الصلة لضمان الجاهزية للتدقيق.

34-17 الأمان

- 1- يجب تضمين تقييم هيكلي يتم إجراؤه خلال مرحلة SDLC لتحديد ومعالجة المخاطر الأمنية المحتملة والثغرات الأمنية ونقاط الضعف المعمارية قبل كتابة التعليمات البرمجية (يُشار إليها باسم "مراجعة تصميم الأمان") في SDLC مع توفر ضوابط وقائية وكشفية تتماشى مع معايير الصناعة مثل OWASP.
- 2- يجب تطبيق ممارسات التشفير الآمنة.
- 3- يجب على المورد تضمين ضوابط أمن المعلومات في عملياته وإجراءاته من أجل اختيار التطبيقات والمنتجات والخدمات وتطويرها وتنفيذها.
- 4- يجب أن يكون لدى المورد إجراء بنية أمن لجميع الأنظمة التي يتم فيها تخزين معلومات Citi و/أو معالجتها و/أو نقلها، ويجب الاحتفاظ بصورة آمنة أو قالب أمن لجميع الأنظمة.

35-17 ضوابط الحماية من تهديدات البرامج الضارة

- يجب على المورد ضمان تنفيذ الضوابط اللازمة لمنع واكتشاف إدخال أي تعليمات برمجية ضارة (مثل الفيروسات العامة أو الفيروسات المتنقلة أو فيروسات حصان طروادة أو برامج الإعلانات المتسللة أو برامج التجسس أو برامج الفدية أو أي هجمات إلكترونية مماثلة يمكن أن يتم من خلالها اختراق البيانات). يجب على المورد:
- 1- تطبيق وتحديث وصيانة تقنية لمكافحة الفيروسات وبرامج التجسس على جميع أجهزة الحاسوب الشخصية وتقنية على جميع خوادم الشبكة المحلية (LAN) وخوادم البريد وغيرها من الأجهزة التي تخزن و/أو تعالج و/أو تنقل بيانات Citi.
 - 2- نشر إعدادات أمان لمنع المستخدمين النهائيين من تعطيل أدوات مكافحة الفيروسات/مكافحة البرامج الضارة وعمليات الفحص المجدولة.
 - 3- وضع إجراءات آلية مُدارة مركزياً لتهينة وتحديث برامج مكافحة الفيروسات ومكافحة البرامج الضارة.
 - 4- التأكد من تنفيذ العمليات لتحديد ومعالجة أجهزة الكمبيوتر غير المتوافقة التي تكون فيها برامج مكافحة الفيروسات أو محركات الفحص قديمة.
 - 5- التحكم في الوصول إلى منافذ/واجهات التواصل التي تسمح بالاتصال بالأجهزة الخارجية بما في ذلك على سبيل المثال لا الحصر وسائط التخزين.

36-17 ضوابط الحماية من التعليمات البرمجية المتنقلة

- يجب على الموردين ضمان تطبيق ضوابط تتعلق بممارسات أمان التعليمات البرمجية المتنقلة. عند الترخيص باستخدام التعليمات البرمجية المتنقلة، يجب أن يفي التكوين، كحد أدنى، بجميع معايير الصناعة ذات الصلة والالتزامات التعاقدية مع Citi، ويجب على المورد ضمان تشغيل التعليمات البرمجية المتنقلة المرخصة وفقاً لسياسة أمنية محددة وموثقة بوضوح، ومنع تنفيذ التعليمات البرمجية المتنقلة غير المرخصة.
- بالنسبة للتعليمات البرمجية المتنقلة التي قد تؤثر على نظام التشغيل الأساسي أو المنصة (أي خارج "آلية تحديد الوصول SANDBOX")، يجب على المورد التحقق من الآتي:

- 1- يجب أن تكون التعليمات البرمجية المتنقلة التي ينشرها المورد تحمل توقيع سلطة إصدار الشهادات المعتمدة لدى Citi ويجب أن تتم إدارة صلاحية الشهادة من قبل المورد لمعالجة انتهاء سريان الشهادة أو دورانها.
- 2- يجب إزالة التعليمات البرمجية المتنقلة الموقعة التي انتهى سريان شهاداتها من الإنتاج.

37-17 تسجيل التدقيق

- يجب على المورد ضمان أن تكون كل نظم المعلومات الخاضعة للسيطرة والمستخدم للوصول إلى بيانات 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:
- 1- الإجراءات المتعلقة بأمان البنية التحتية للمنصة المرتبطة
 - 2- جميع إنذارات النظام المرتبطة بجدار الحماية أو نظام كشف التسلل/نظام منع التسلل التي أوجدت الحدث الأمني
 - 3- جميع محاولات انتهاك أمان النظام (مثل المحاولات الفاشلة لتسجيل دخول المستخدم)

- 4- محاولات غير مصرح بها للوصول إلى الموارد (البرامج والبيانات والعمليات وما إلى ذلك)
- 5- إجراءات المسؤول
- 6- المعلومات المتعلقة باستقبال معلومات محددة من مستخدم أو نظام آخر
- 7- جميع الأحداث المهمة المتعلقة بالمعاملات المالية ومعلومات Citi التي تتضمن على وجه التحديد العناصر التالية:
 - (أ) تحديثات المعاملات المالية
 - (ب) تحديثات بيانات معلومات PII السرية أو الحساسة
 - (ج) تحديثات البيانات المقيدة
 - (د) تحديثات بيانات المصادقة
- 8- جميع الجلسات التي تم إنشاؤها
- 9- يجب الحصول على أدوات الإنترنت خلال فترة الاتصال مثل مُعرّف الجهاز الفريد، عندما يكون ذلك ممكناً من الناحية الفنية، وتسجيلها من أجل تطبيقات Citi المواجهة (أي المواقع الإلكترونية وتطبيقات الأجهزة الجوال) لدعم عمليات التحقق في الاحتيال. يجب أن تتضمن هذه الأدوات كحد أدنى عناوين IP. يجب الحصول على هذه الأدوات لمعاملات Citi ولنشاط فتح حساب لدى Citi. يجب أن تُجمع المعلومات حتى يمكن ربط أدوات فترة الاتصال بالمعاملة أو فتح الحساب.
- 10- يجب أن توثق مسارات التدقيق نسبة نشاط معين إلى فرد معين لمنع التنصل من النشاط.
- 11- يجب تسجيل الأحداث المهمة الخاصة بإدارة أمن المعلومات (ISA) تحديداً بما في ذلك العناصر التالية:
 - (أ) إنشاء حساب المستخدم
 - (ب) تعديل حقوق الوصول الخاصة بالمستخدم
 - (ج) حذف وإنشاء وتعديل ملفات التعريف لنظام معلومات خاضعة للسيطرة
 - (د) عمليات إعادة تعيين كلمة المرور
 - (هـ) التغييرات التي تطرأ على تكوين أمن النظام
 - (و) جميع الأنشطة التفاعلية للمُعرفات (IDs) الوظيفية المميزة
 - (ز) يجب أن تحتوي سجلات الأمان على المعلومات التالية على الأقل بغض النظر عن النظام الذي يُنشئ السجل، إلا إذا كان ذلك التضمين غير ممكن من الناحية الفنية:
 - 1- تاريخ ووقت الحدث (بالتوقيت العالمي الموحد UTC)
 - 2- هوية (ID) المستخدم للشخص الذي يقوم بالإجراء
 - 3- نوع الحدث
 - 4- اسم الأصل أو المورد المتأثر
 - 5- نوع الوصول (حذف، تعديل، وما إلى ذلك)
 - 6- نجاح الحدث أو فشله
 - 7- المصدر (محطة طرفية، منفذ، موقع، عنوان IP، اسم المضيف، وما إلى ذلك)

38-17 حماية معلومات السجل

- يجب على المورد التأكد من تنفيذ ضوابط الوصول للحفاظ على سلامة مسارات التدقيق أثناء البدء والإغلاق وأثناء التخزين والنقل.
- 1- لمنع التعديلات غير المصرح بها في سجلات التدقيق، يجب على المورد التأكد من أن السجلات لا يمكن التعديل عليها بالكتابة أو تعديلها من قبل مستخدمي النظام الذين يقومون بتتبع نشاطهم.
 - 2- يجب على المورد تزويد Citi بإجراءات الاحتفاظ بالسجلات لبيانات السجلات التي تحدد كيفية الاحتفاظ بالبيانات وتتضمن تدابير الامتثال التي تشير إلى جميع المتطلبات القانونية والتنظيمية المعمول بها.
 - 3- يجب أن تكون ساعات جميع أنظمة معالجة المعلومات ذات الصلة داخل المؤسسة أو المجال الأمني متزامنة مع مصدر زمني دقيق.

39-17 استخدام نظام الرصد

- يجب على الموردين التأكد من التقاط الأحداث التالية وتسجيلها ومراجعتها بشكل مباشر أو من خلال عملية مراجعة آلية:
- 1- جميع إنذارات النظام المرتبطة بجدار الحماية أو نظام كشف التسلل (IDS)/نظام منع التسلل (IPS) التي أوجدت الحدث الأمني.

- 2- جميع التحديثات للموارد المهمة كما هو محدد في البنية القياسية الأمانة.
- 3- جميع الأنشطة التفاعلية التي يتم تنفيذها من خلال أي معرفات (وظيفية أو مميزة أو نظامية أو مؤقتة، وما إلى ذلك) مع إمكانية الوصول إلى المعلومات المصنفة على أنها معلومات PII سرية أو عليا.
- 4- أحداث ISA المهمة الواردة في قسم تسجيل التدقيق أعلاه مع الاستثناء التالي:
 - أ) إزالة الاستحقاقات من المستخدم أو الدور أو ملف التعريف إذا تم تنفيذ نشاط إدارة أمن المعلومات عن طريق نظام آلي لسير العمل/التنفيذ يحتوي على ضوابط سلامة شاملة.

40-17 معرف ارتباط السجل والمراجعة

- 1- عندما يؤدي حدث مسجل إلى استدعاء تنبيه، وتتم مراجعة الحدث، يجب على المورد البدء في اتخاذ إجراءات متابعة وإجراء تحقيقات، إذا كان هناك مؤشر على احتمالية وقوع حادث ضار بشأن أمن المعلومات.
- 2- يجب أن يضمن المورد أن تكون سجلات التدقيق مُجمعة في نظام إدارة سجلات مركزي مثل نظام معلومات الأمن وإدارة الأحداث (SIEM) أو أداة تحليل السجلات لتحليل ارتباط السجل ومراجعته.
- 3- يجب على الموردين مراجعة وضبط تهيئة نظام SIEM الخاص بهم أو أداة تحليل السجلات بصفة دورية لتحسين عملية تحديد الأحداث القابلة للتنفيذ.

41-17 التحكم في برامج التشغيل

- يجب على المورد ضمان ألا يستخدم سوى أنظمة التشغيل والبرامج المدعومة حاليًا من قبل مزود تجاري معتمد في هذا المجال، أو التي تُصدر بانتظام وبشكل مناسب تحديثات أمنية وتصحيحات للتكوين لمعالجة الثغرات الأمنية.
- يجب على المورد ضمان تنفيذ عملية موثقة تحدد الأطر الزمنية للمعالجة التي يتم خلالها تطبيق جميع تصحيحات وتكوينات الأمان المعتمدة.
- بغض النظر عن أي اتفاقية صيانة منفصلة بين المورد و Citi، يجب على المورد التأكد من أن البرامج التي تم تطويرها لصالح Citi والمحكومة بموجب اتفاقية ترخيص لا تسمح باستخدام إصدارات من البرامج غير المدعومة التي تكون بها ثغرات أمنية معروفة، وأنه يتم تحديث تلك البرامج وتصحيحها عند اللزوم في الوقت المناسب.
- يجب الحصول على برامج التطبيقات المستخدمة في معالجة معلومات Citi من موردين معتمدين ويجب أن تكون مرخصة ومفهرسة ومدعومة.

42-17 إدارة المخاطر والثغرات الأمنية

- 1- يجب على المورد تنفيذ عملية إدارة الثغرات الأمنية والتهديدات التي تعالج و/أو تتضمن بشكل شامل كل ما يلي:
 - أ) أدوات وإجراءات اكتشاف الثغرات الأمنية وإدارتها لكل الأصول التي يمكن أن تُستخدم لمعالجة بيانات Citi السرية أو العليا أو تخزينها أو الوصول إليها أو نقلها.
 - ب) اشتراط إجراء عمليات فحص أسبوعية على الأقل باستخدام أدوات ومنهجيات معترف بها في القطاع لتحليل الثغرات الأمنية وإعداد التقارير.
 - ج) تصنيف الثغرات الأمنية وفقًا لأحدث إصدار من "Common Vulnerability Scoring System (CVSS)" (انظر <https://www.first.org/cvss>)، مع أطر زمنية تصحيحية بناءً على مدى خطورتها.
 - د) شرط اختبار عمليات علاج الثغرات الأمنية قبل نشر الإنتاج بالكامل.
 - هـ) عملية تشغيلية موثقة وقابلة للتكرار لتسريع معالجة الثغرات الأمنية الحرجة.
 - و) يجب على المورد تتبع الأصول طوال دورة حياتها القابلة للدعم استعدادًا لحالات انتهاء العمر الافتراضي (EOL) أو انتهاء دعم المورد (EOVS)، كما يجب أن يكون لديه إجراءات مطبقة للقيام بشكل استباقي بترقية هذه الأصول أو استبدالها.
 - ز) يجب إعطاء أولوية لأي CVSS حرجة يتم تحديدها من خلال جمع المعلومات أو عمليات مسح الثغرات أو اختبار الاختراق ومعالجتها ضمن إطار زمني محدد تحديدًا جيدًا يتناسب مع مخاطر تلك الثغرات.

إذا كان المورد يحتفظ ببيانات Citi السرية أو الأكثر حساسية أو تخزنها على موقع ويب أو نظام يمكن الوصول إليه عبر الإنترنت، أو موقع ويب يحمل علامة Citi التجارية، ففي هذه الحالة ومن أجل الحماية من أي ثغرة أمنية أو تهديد مما ينطوي على منتجات أو خدمات تؤثر على Citi (يُشار إليها باسم "ثغرة أمنية")، يجب على المورد الامتثال للمتطلبات التالية:

- 1- تعيين موظف من جانب المورد للرد على استفسارات Citi المتعلقة بأمن المعلومات.
- 2- استخدام أفضل الممارسات المعترف بها في المجال، بصفة أسبوعية على أقل تقدير، لرصد المصادر حسنة السمعة فيما يتصل بالمعلومات حول ثغرات أمن الكمبيوتر مثل FIRST و CERT/CC وكتالوج الثغرات الأمنية المستغلة المعروفة من قبل CISA والقوائم البريدية للبائعين، واتخاذ التدابير المناسبة للحصول على حزم الخدمة والتصحيحات والترقيات والحلول البديلة ذات الصلة واختبارها بشكل كامل وتطبيقها وتقديمها إلى Citi.
- 3- اختبار تنفيذ تدابير أمن المعلومات، على أساس ربع سنوي على الأقل، باستخدام أدوات فحص الثغرات الأمنية في الشبكة والنظام والتطبيق و/أو اختبار الاختراق.
- 4- السماح لـ Citi أو لطرف ثالث معتمد من Citi بالقيام في أوقات زمنية معقولة بإجراء تقييمات للثغرات الأمنية أو الاختراقات الأخلاقية أو أي تقييمات أمان أخرى، للتحقق من امتثال المورد للالتزامات بموجب أي عقد وبموجب هذه المتطلبات، بما في ذلك على سبيل المثال لا الحصر، مراجعة السياسات والعمليات والإجراءات، والتقييمات في الموقع لترتيبات الأمان المادي، ومسح الثغرات الأمنية في الشبكة، والنظام، والتطبيقات، واختبار الاختراق، باستخدام الأدوات المتاحة تجاريًا و/أو الممارسات القياسية في المجال لإجراء عمليات الفحص هذه.
- 5- يجب أن يكون أي مقال يقدم خدمات تقييم الثغرات الأمنية للمورد مدرجًا في قائمة مزودي خدمات تقييم الثغرات الأمنية المعتمدة لدى Citi. وفي حال استعانة المورد بمقاولين أو مقاولين من الباطن لتقديم الخدمات، يجب على المورد، وعلى نفقته الخاصة، ضمان إتمام أي تقييمات مطلوبة للثغرات الأمنية، وذلك بنفس الطريقة وفي الوقت المناسب كما لو كان المورد هو من يقدم تلك الخدمات مباشرة، كما يجب أن يضمن توثيق شرط تكليف أي مقاول أو مقاول فرعي بتسهيل هذه التقييمات في الاتفاقية المبرمة بين المورد والمقاول/المقاول من الباطن فيما يتعلق بالخدمة، بما في ذلك الصياغات اللغوية والنصوص التي تحوّل Citi بإجراء تلك التقييمات.
- 6- الإخطار.
 - أ) عندما يحدد المورد وجود ثغرة أمنية تتعلق بمنتج أو خدمة تؤثر على Citi، يجب على المورد إخطار Citi كتابيًا في غضون 24 ساعة من وقوفه على تلك الثغرة، وأن يضمن إخطاره وصفًا للإجراءات العلاجية التي يتخذها المورد.
 - ب) عندما يدرك المورد وجود ثغرة أمنية تنطوي على منتج أو خدمة تؤثر على Citi عقب الإفصاح العام المسؤول عن قنوات العملية (نشر الثغرة الأمنية في قاعدة بيانات الثغرات الوطنية (NVD) أو عبر كتالوج التهديدات المقدم إلى مزودي الحلول الأمنية الخارجيين)، يقوم المورد بإخطار Citi كتابيًا خلال 24 ساعة من تاريخ ذلك النشر. سوف يحتوي كل إخطار على معلومات حول الثغرة الأمنية، وما إذا كانت الثغرة تؤثر على Citi، وفائدة النظام للخدمات المتعلقة بـ Citi (أي ما إذا كان يستضيف معلومات Citi أو يُستخدم في تقديم الخدمات أو كليهما)، وما إذا كان من الممكن استغلالها عن بُعد؛ ودرجة الثغرة وفق نظام Common Vulnerabilities and Exposures (CVE). سوف يستمر المورد في تقديم التحديثات إلى Citi حتى يتم إصلاح الثغرة الأمنية. وفي الحالات التي يقف فيها Citi على ثغرة أمنية، يمكن لـ Citi تقديم إشعار بهذا الخصوص إلى المورد، ويجب على المورد معالجة هذه الثغرة على الفور وفقًا لهذا القسم.

- 7- المعالجة. بالنسبة لكل ثغرة أمنية يتم تقديمها بموجب هذا القسم، سيقوم الطرف المُخطر بتقييم مستوى المخاطر وتأثير تلك الثغرة بناءً على شدتها ومخاطرها على Citi وتعيين مستوى أولوية للمخاطر بناءً على نظام Common Vulnerability Scoring System (CVSS) على النحو المنصوص عليه في الملحق (أ) لذلك النظام، (انظر <https://www.first.org/cvss>). بمجرد تعيين مستوى المخاطر والاتفاق

عليه من جانب الطرفين، يقوم المورد بمعالجة أي ثغرة متوسطة أو عالية أو حرجية تم تحديدها. حيثما أمكن، يجب توفير الإصلاح لأي ثغرة أمنية ضمن حزمة أمان فيما يتصل بالإصدار المنشور حالياً.

إذا كان المورد غير قادر أو غير راغب في معالجة الثغرة الأمنية على النحو الذي يرضى عنه Citi، فيجوز لـ Citi إنهاء الترخيص ذي الصلة دون أي مسؤولية أخرى أو التزام مالي (بالنسبة للجزء الذي تم فسخه)، ويجب على المورد أن يرد إلى Citi على الفور ذلك الجزء من رسوم الترخيص المدفوعة بالنسبة والتناسب.

44-17 ضوابط شبكة أمان الاتصالات

1- يجب أن تكون شبكات المورد 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 نقاط التنفيذ في الشبكة.

- (أ) يجب ألا يتم تخزين المعلومات المصنفة على أنها من معلومات Citi السرية أو العليا باستمرار على نظام يوجد بمنطقة آمنة مراقبة (DMZ) مواجهة للإنترنت. يمكن أن تكون الشبكات المستخدمة للوصول إلى معلومات Citi و/أو تخزينها و/أو إدارتها و/أو معالجتها و/أو نقلها باستخدام الشبكات المحلية اللاسلكية (WLAN) أو غيرها من حلول الأجهزة اللاسلكية التي تتضمن عناصر تحكم معقولة لحظر الوصول غير المصرح به (EAP-PEAP-TLS أو TTLS، وما إلى ذلك) بالشبكات التي تحتوي على معلومات Citi.
- (ب) جميع اتصالات IP الخارجية الموصلة إلى الشبكة العالمية للموردين محمية ببرنامج جدار وقائي للحماية يديره المورد.
- (ج) تطبيق نظام لكشف التسلل (IDS) في الوقت الحقيقي أو نظام لمنع التسلل (IPS) يراقب ويحمي اتصالات الإنترنت بشبكة المورد التي يتم فيها الوصول إلى معلومات Citi أو إدارتها أو تخزينها أو معالجتها أو نقلها.

2- بالنسبة لجميع تطبيقات الإنترنت التي تحمل علامة Citi التجارية، يجب على المورد التأكد من:

- (أ) حماية الخدمات المستضافة في مواقع المورد من خلال خدمات مكافحة رفض الخدمة الموزعة (DDoS) المعتمدة من Citi أو عناصر تحكم مماثلة خضعت للتحقق منها بواسطة Citi.
- (ب) وجوب تهيئة جدران حماية خارجية بقاعدة للرفض افتراضياً. وجوب تهيئة قواعد برامج الحماية على أساس مبدأ الامتياز الأقل وجوب تسجيل كل محاولات الاتصال المرفوضة بواسطة جدار الحماية (مثل إفلات حزم البيانات).
- (ج) وجوب رفض حركة اتصالات الشبكة بشكل افتراضي والسماح بها على نحو استثنائي في الواجهات المدارة. وجوب كون الاستثناءات محدودة للغاية بحيث تقتصر على مصادر ووجهات وخدمات محددة.
- (د) وجوب احتواء حركة مرور تطبيقات الويب على ضوابط مناسبة وتصفيته، على سبيل المثال من خلال جدران حماية تطبيقات الويب.

45-17 الفصل داخل الشبكات

يجب على المورد 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 بالمورد.

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

يتطلب الوصول عن بُعد وأمن المضيف تنفيذ ضوابط التحكم في وصول القائمة على المجموعة (مثل الموظفين والمقاولين من الباطن) لتقييد الوصول إلى موارد الشبكة ضمن شبكة المورد. على مستوى المضيف، يمكن تطبيق التحكم في الوصول على مستوى المجموعة أو الفرد.

46-17 تحديد الأجهزة في الشبكات

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

- 1- لا يجوز الوصول إلى شبكة Citi التي يتم تخزين المعلومات عليها أو معالجتها أو نقلها إلا من خلال أجهزة المورد (أي أجهزة الهاردوير، بما في ذلك، على سبيل المثال لا الحصر: أجهزة الحاسوب المكتبية وأجهزة الحاسوب المحمولة) التي تمتثل لهذه المتطلبات والمصرح بها من قبل المورد.
- 2- يُحظر الوصول إلى شبكة Citi إلا على أجهزة المورد (أي أجهزة الهاردوير، 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.

47-17 تحليل وتوصيف متطلبات الأمان

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

48-17 المعاملات عبر الإنترنت

- 1- عند الاقتضاء، يجب أن يكون لدى المورد نظم معلومات تستخدم كلمات مرور ديناميكية أو شهادات رقمية للتحقق من صحة بيانات الاعتماد.
- 2- يجب استبدال جميع شهادات الكيان النهائي مرة واحدة على الأقل كل 13 شهرًا.
- 3- يجب على تطبيقات الموردين 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:
 - (أ) استخدام طريقة مصادقة قائمة على أنواع البيانات/الوظائف التي يتم الوصول إليها؛
 - (ب) إجراء تقييم امتثال للمصادقة متعددة العوامل (MFA) وتنفيذ التوصيات إذا لزم الأمر؛
 - (ج) إجراء تقييم أولي لمراقبة الأنشطة المشبوهة (SAM) وتنفيذ التوصيات إذا لزم الأمر؛
 - (د) في كل الحالات، ينبغي على المورد الاتصال بجهة الاتصال الرئيسية للأعمال للتعرف على متطلبات Citi الحالية.

49-17 إجراءات التحكم بالتغيير

- 1- يجب على المورد ضمان توجيه تغييرات التكوين التي تطرأ على جدران الحماية وأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) عبر عملية إدارة التغيير الخاصة بالمورد.
- 2- ويجب تسجيل الدخول الممنوح للإنتاج من خلال معرفات مؤقتة ورصده من أجل تتبع التغييرات التي يتم إجراؤها في البيئة.
- 3- 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 للقسمة 32-17 (تسجيل التدقيق) بواسطة المورد. ويجوز أن تستند تلك المراجعات إلى منهجية مناسبة من منهجيات أخذ العينات القائمة على المخاطر.
- 4- ويجب أن تتحقق المراجعة من أن التغييرات التي تعتبر جزءًا من الوصول المميز المؤقت قد تم إجراؤها على النحو المنشود.
- 5- يجب على المورد توثيق جميع التغييرات، بما في ذلك تخزين الأدلة على عملية المراجعة.

50-17 تسريب المعلومات

يجب أن يكون لدى المورد معيار موثق للترميز الآمن يهدف إلى يمنع تسريب المعلومات، بما في ذلك:

- 1- معلومات مفصلة عن النظام (مثل نوع الخادم والتكنولوجيا).
- 2- عمليات تتبع التكدس وأخطاء الاستثناء التي تكشف عن بنية هيكل الدليل ونوع قاعدة البيانات الأساسية.

51-17 بيانات الاختبار

لا يجوز للمورد استخدام أو تخزين المعلومات السرية أو العليا على النحو المحدد من قبل Citi في بيانات تطوير أو اختبار تطبيق (تطبيقات) البرامج أو المختبرات ما لم يتم إلغاء تحديد هذه المعلومات و/أو إخفاؤها و/أو تشويشها باستخدام الأدوات والطرق التي تفي بمعايير الصناعة بحيث لا تعود تلك البيانات حساسة، أو يجب على المورد تنفيذ ضوابط تحكم الإنتاج المباشر ضمن بيانات التطوير أو الاختبار.

52-17 قبول النظام

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

53-17

الإبلاغ عن مواطن الضعف في أمن المعلومات

يجب أن يطبق المورد عملية تضمن **إبلاغ Citi على الفور** بأي نقاط ضعف في التطبيقات والبنية التحتية قد تؤدي إلى الإضرار بأصول معلومات Citi.

54-17

المسؤوليات عن الحوادث الأمنية والإجراءات المتخذة حيالها

1- إن عبارة عن حدث أمني يُعرض أيًا مما يلي للخطر، بغض النظر عن كيفية وقوع الحادث الأمني أو مكانه، أو من الذي يحتمل أن يكون قد تسبب في هذا الاختراق:

- سرية بيانات Citi أو سلامتها أو توافرها.
 - سرية أو سلامة أو توافر أي بيانات (بما في ذلك المعلومات الشخصية) التي يخضع Citi فيما يتعلق بها للالتزامات تعاقدية أو قانونية أو تنظيمية.
 - سلامة أو توافر أنظمة معلومات Citi التي تخزن أو تعالج أو تنقل أي بيانات تخص Citi.
- 2-** لأغراضنا، يشير اصطلاح انتهاك السرية إلى تعرض البيانات للاختراق من جانب شخص غير مصرح به، أو من خلال سيناريوهات يفقد فيها Citi حيازته للبيانات والتحكم فيها. ويجب الإبلاغ عن جميع الحوادث الأمنية على الفور.
- 3-** في حالة تعرض المورد لحادثة SIRT، فيجب على المورد التعاون مع Citi في تقديم المعلومات التي يطلبها Citi وفقًا لعمليات الاستجابة للحوادث الخاصة بـ Citi، وتحليل البيانات المخترقة بطريقة كافية بما يسمح لـ Citi بتلبية متطلبات الحوكمة القانونية و/أو التنظيمية و/أو الداخلية؛ وتقديم أي/كل الإخطارات المطلوبة بموجب القانون أو القواعد أو اللوائح المطلوبة من قبل Citi على أساس تقديري وبناء على طلب Citi وعلى نفقة المورد، وبعد أن تتاح لـ Citi الفرصة لمراجعة وتعديل صياغة نموذج الإخطار المقترح؛ ويجب على المورد عدم ذكر اسم Citi في أي من هذه الإخطارات ما لم يطلب Citi تحديدًا أن تتم تسميته كتابة.

55-17

الحماية ضد تسريب البيانات (DLP)

يجب أن يطبق المورد ضوابط تفادي تسريب البيانات (DLP)، بما في ذلك مراقبة المحتويات والنقاط النهائية التي تغطي كل الموظفين الذين يمكنهم الوصول إلى بيانات Citi السرية أو العليا. يجب أن يكون لدى المورد ضوابط قائمة لاكتشاف و/أو منع حالات تسرب بيانات Citi السرية أو العليا خارج شبكته عبر القنوات التالية:

- أ) رسائل البريد الإلكتروني غير المشفرة
- ب) مرفقات البريد الإلكتروني غير المشفرة
- ج) طباعة بيانات Citi
- د) نقل بيانات Citi إلى مواقع خارج شبكته (على سبيل المثال عبر FTP)
- هـ) 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. يجب منع هذا الامتياز افتراضيًا.
- و) يجب أن يشمل حل تفادي تسريب البيانات (DLP) إرسال سجل وتنبيه إلى المورد بكل الأحداث التي تمثل محاولات (ناجحة أو محظورة) لنقل أو تحويل أو نسخ بيانات Citi السرية أو العليا من شبكته إلى جهات أخرى. يجب منع هذا الامتياز افتراضيًا.
- ز) تحميل بيانات Citi إلى مواقع الويب الخارجية، بما في ذلك مواقع البرمجيات كخدمة (SaaS)/مواقع مشاركة الملفات. يجب منع هذا الامتياز افتراضيًا.

- 1- يجب أن يكون لدى المورد 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.
- 2- أما بالنسبة للموردين الذين يمكنهم الوصول إلى بيانات Citi السرية أو العليا:
 - (أ) يجب تسجيل كافة طلبات عناوين URL.
 - (ب) 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، والذكاء الاصطناعي التوليدي (Gen-AI)، وما إلى ذلك).
 - (ج) يجب حظر الوصول إلى المواقع التي من شأنها أن تعرض البيئة إلى تهديدات البرامج الضارة أو الهجمات.
 - (د) يجب حظر محاولات الوصول إلى المواقع التي تعتبر غير مرتبطة بالعمل.
 - (هـ) يجب على المورد الاشتراك في خدمة تصنيف عناوين URL التي يتم تحديثها بانتظام؛ حيث يتم افتراضياً حظر كل عناوين URL غير المصنفة أو يتم حظر كل عناوين URL بشكل افتراضي ويتم اعتمادها على أساس كل حالة على حدة.
 - (و) يجب أن يتم دعم متصفحات الويب التي يستخدمها المورد دعماً كاملاً وأن يتم تحديثها وفقاً لآخر تحديثات الأمان بواسطة مورد البرامج.

57-17 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 المورد أو الشبكات التي تحتوي على معلومات Citi، ما لم يتم تطبيق تشفير ملائم على جميع بيانات Citi وفقاً للقسـم 9-17 (سياسة استخدام ضوابط التحكم التشفيرية).

58-17 البريد الإلكتروني

- يجب أن يكون لدى المورد ضوابط قائمة خاصة بالبريد الإلكتروني لمنع مشاركة معلومات Citi والتعرض لتهديدات البرامج الضارة أو الهجمات. ويشمل ذلك ما يلي:
- 1- يتم فحص مرفقات الملفات الواردة التي تدخل بوابة البريد الإلكتروني ويتم حظرها إذا كانت تشكل خطراً على النظام.
 - 2- برنامج تصفية البريد الإلكتروني (مكافحة البريد الإلكتروني العشوائي، مكافحة التصيد الاحتيالي) قيد الاستخدام ومُحدَّث.
 - 3- يجب تشفير أي بيانات سرية أو عليا لدى Citi عند إرسالها خارج مؤسسة المورد.
 - 4- يتم دعم عملاء البريد الإلكتروني التي يستخدمها المورد دعماً كاملاً ويتم تحديثها وفقاً لآخر تحديثات الأمان التي يوفرها بائع البرامج.

59-17 الوسائط القابلة للإزالة

- 1- يجب على المورد حماية معلومات Citi بغض النظر عن الوسائط المحتفظ بالمعلومات عليها. ينطبق هذا المعيار، على سبيل المثال لا الحصر، على الأنواع التالية من الوسائط التي تكون المعلومات مخزنة عليها: 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.
- 2- 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.
- 3- إذا كان مسموحاً باستخدام الوسائط القابلة للإزالة، فهذا الاستخدام يجب أن يخضع لعملية موافقة الإدارة، بما في ذلك منطوق الأعمال الذي يتطلب استخدام الوسائط القابلة للإزالة. يجب عمل قائمة بالوسائط القابلة للإزالة بواسطة الإدارة. يجب تشفير الوسائط القابلة للإزالة التي تشمل بيانات Citi السرية أو العليا تلقائياً دون إلزام المستخدم بأي إجراء.

- 1- عندما تصير معلومات Citi المصنفة على أنها سرية أو عليا مؤهلة للتخلص منها وفقاً للتعليمات المقدمة من Citi (أي عندما لا تصبح المعلومات مطلوبة من قبل Citi أو مفيدة له، وبعد انقضاء أي فترة استبقاء إضافية تفرضها القوانين و/أو اللوائح و/أو سياسات Citi)، يجب على المورد إتلاف هذه المعلومات بطريقة تجعلها غير صالحة للاستعمال وغير قابلة للاسترداد.
- 2- يجب استخدام أداة معتمدة تستبدل عشوائياً قطاعات الأقراص بأحرف معينة ومختلفة لمسح الوسائط القابلة للتركيب بشكل آمن بناءً على القواعد التالية:
 - (أ) بالنسبة للوسائط التي تخزن معلومات مصنفة باعتبارها سرية أو عليا، يجب أن تستكمل الأداة ثلاث عمليات مسح للوسائط.
 - (ب) إزالة المغنطة من الوسائط (حسب الاقتضاء).
- 3- إتلاف الوسائط فعلياً لجعلها غير صالحة للقراءة (أي فرم الأوراق، تكسير الأقراص).
- 4- يجب تجميع وسائط التخزين الورقية وغير الإلكترونية الأخرى التي تشمل معلومات سرية أو عليا وتخزينها في "حاوية سرية" آمنة قبل التخلص منها نهائياً. يجب أن تكون الحاويات السرية مغلقة دائماً ولا يمكن فتحها إلا من قبل الموظفين المصرح لهم.
- (أ) يجب كذلك حذف المعلومات من أجهزة التصوير والفاكس والطابعات وأي أجهزة أخرى بها ذاكرة/سعة تخزين قد تشمل معلومات سرية أو عليا تخص Citi.

61-17 إدارة أمن المعلومات والتدريب

- 1- وضع برنامج توعية وتعليم مناسب حول الأمان السبراني/أمن المعلومات يتضمن، على سبيل المثال لا الحصر، منع التصيد الاحتيالي وهجمات الهندسة الاجتماعية الأخرى، والتعامل المناسب مع المعلومات السرية أو العليا، والإبلاغ عن الحوادث الأمنية وإدارة الاستجابة.
- 2- يجب أن يضمن المورد حصول كل الموظفين، بما في ذلك المقاولين والموظفين المؤقتين، على التعليم والتدريب التوعوي الملزم حول السياسات والإجراءات التنظيمية ذات الصلة بمهامهم الوظيفية.
- 3- يجب على المورد ضمان مراجعة وتحديث البرنامج التدريبي والتوعوي سنويًا لمعالجة المخاطر والتهديدات الناشئة وأفضل الممارسات الحالية والتقنيات الجديدة في مشهد الأمن السبراني.
- 4- وكحد أدنى، يجب أن يتضمن المواضيع التالية:
 - (أ) التمييز بين المعلومات والتعامل معها
 - (ب) النقل الآمن (بريد إلكتروني آمن، مخزن SharePoint آمن، عدم إرسال بيانات مملوكة لدى Citi إلى بريد إلكتروني شخصي)
 - (ج) الإبلاغ عن الحوادث المتعلقة بأمن المعلومات
 - (د) مكان عمل آمن (مثل الاستخدام المناسب للإنترنت، البرامج غير المصرح بها، حظر تنزيل البرامج غير المعتمدة)
 - (هـ) إدارة كلمات المرور (مثل استخدام كلمات المرور القوية، حظر مشاركة كلمات المرور)
 - (و) الهندسة الاجتماعية (مثل التصيد الاحتيالي، والتصيد الموجه، والتصيد الصوتي، والتصيد عبر الرسائل النصية القصيرة)
 - (ز) العمل عن بُعد (مثل الاتصال الآمن/الموثوق، أمان الجهاز الشخصي)
- 5- يجب تكليف موظفي المورد بالتدريب بمجرد حصولهم على حق الوصول إلى الأنظمة التي تستضيف بيانات Citi أو قبل ذلك، واستكمال التدريب في التاريخ المحدد في إخطار التكليف.
 - (أ) ينبغي توفير التدريب على نظم المعلومات (IS) لجميع الموظفين بصفة سنوية على الأقل ما لم يحظر القانون ذلك.
- 6- ينبغي أن يتضمن التدريب أداة لتقييم فعاليته (مثل اختبار قصير عند الانتهاء مع تحديد معيار للنجاح أو الرسوب) حيثما تسمح القوانين المحلية بذلك.

62-17 برنامج إدارة المخاطر السبرانية

- يجب على المورد أيضًا، وكحد أدنى، توفير برنامج مناسب لإدارة المخاطر السبرانية يتضمن، على الأقل، ما يلي:
- 1- وضع برنامج لإدارة مخاطر أمن المعلومات محدد تحديدًا جيدًا وموثق و/أو برنامج لإدارة مخاطر التشغيل يحتوي على مكون محدد بوضوح لإدارة المخاطر السبرانية/المعلوماتية، والذي يحدد المستوى المقبول لدى المورد من المخاطر السبرانية ويضمن أن المخاطر السبرانية المتبقية تتوافق مع ذلك المستوى المقبول من المخاطر.
 - 2- وضع 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 سنويًا على الأقل إلى قيادتها التنفيذية للمراجعة والتأكد من عدم انتهاك المستوى المقبول من المخاطر السبرانية لدى المورد.
 - 3- ضمان الامتثال لأي معايير PCI Data Security Standards (PCI-DSS) المطبقة على المورد حيث يقوم المورد بمعالجة و/أو تخزين و/أو نقل معاملات بطاقات الائتمان/الخصم و/أو المدفوعات و/أو المعلومات.
 - 4- وضع خطة لإدارة الأزمات ودليل لفريق الاستجابة للحوادث الأمنية بما يتفق مع معايير الصناعة لضمان أن يتوافر لدى المورد القدرة الكافية والملائمة لاكتشاف أي حادثة أمان سبراني واحتوائها والتحقيق فيها والاستجابة لها والتعافي منها سواء كانت هذه الحادثة مجرد محاولة و/أو اشتباه و/أو كانت حادثة فعلية.

63-17 أمان التطبيقات، و API، والتعليمات البرمجية، وأمان النظام والبنية التحتية

عندما يقوم المورد باستضافة و/أو تطوير و/أو الاشتراك في تطوير و/أو توفير بيانات التطوير و/أو تزويد تطبيق/تطبيقات برمجية، يجب على المورد القيام بمراجعات التعليمات البرمجية للبرنامج المذكور و/أو تصحيحات البرنامج بحثًا عن أي

ثغرات 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 APIs)، إلى جانب خدمات النظام الأساسية وأنظمة 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 إفصاح 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 المورد إلى Citi.

64-17 أمان الأجهزة المحمولة

في حالة قيام المورد بتوفير حل عبر تطبيق للهاتف المحمول، يجب على المورد الامتثال للمتطلبات التالية:

- 1- يجب ألا يدعم تطبيق الهاتف المحمول سوى الإصدارات المتوفرة عموماً (GA) و/أو المستقرة وغير منتهية الصلاحية (non-EOL)² من منصات Google Android (باستثناء Android Go) و/أو Apple iOS/iPadOS. إذا كان حل الهاتف المحمول مجهزاً بدعم لأنظمة/إصدارات إضافية، فسوف تكون أنظمة/إصدارات التشغيل المدعومة قابلة للتكوين من قبل Citi.
 - 2- يجب ألا يدعم حل الهاتف المحمول المنصات/الأجهزة المحمولة غير المجهزة بمجموعات تعليمات منتظمة لدعم خوارزميات التشفير بما في ذلك، على سبيل المثال لا الحصر، التشفير على النحو المحدد في القسم 9-17 (متطلبات التشفير) من هذا المستند.
 - 3- لا يُسمح في بيئة الإنتاج بإصدارات نظام التشغيل ما قبل الإنتاج، بما في ذلك على سبيل المثال لا الحصر الإصدارات/النسخ التجريبية وإصدارات/نسخ الوصول المبكر وإصدارات/نسخ معاينة الميزات.
 - 4- يجب أن يكون المورد قادراً على توفير قائمة بمكونات الطرف الثالث المدمجة بما في ذلك، على سبيل المثال لا الحصر، مكتبات البرمجيات المجانية ومفتوحة المصدر التي يتم تجميعها/الاستفادة منها بواسطة حل الهاتف المحمول.
 - 5- يجب أن يلبي تطبيق الهاتف المحمول المتطلبات وأفضل الممارسات التي تتيح نشر تطبيقات الهاتف المحمول عبر متاجر التطبيقات العامة، مثل متجر تطبيقات Apple App Store أو Google Play Store. وسوف تكون متاجر التطبيقات العامة المدرجة هي الطريقة المفضلة والأساسية لتوزيع/نشر تطبيق الأجهزة المحمولة.
 - 6- يجب أن تستخدم تطبيقات أجهزة Android المحمولة نظام التوقيع APK v2+. يجب عدم استخدام نظام التوقيع APK الإصدار 1 (المعروف أيضاً باسم توقيع JAR).
 - 7- يجب أن يتقيد نوع مفتاح توقيع تطبيق الهاتف المحمول وطوله بالقسم 9-17 - متطلبات التشفير في هذا المستند.
 - 8- يجب إدارة كل مفتاح لتوقيع التطبيقات وشهادة X.509v3 المرتبطة به بشكل فردي ومخصص بمعرف تطبيق واحد/معرف حزمة واحدة. ويجب عدم مشاركة مفتاح (مفاتيح) التوقيع بين التطبيقات.
 - 9- إذا كان تطبيق الهاتف المحمول يتطلب الاحتفاظ بالبيانات على الجهاز المحمول، فيجب ألا يحتفظ إلا بأحدث البيانات على الجهاز مما يكون ضرورياً لغرض (أغراض) التطبيق/الخدمة، أو طالما كان ذلك لازماً وفقاً للمتطلبات القانونية أو التنظيمية.
- أ) يجب أن يتوافق جمع بيانات المستخدم و/أو معالجتها و/أو تخزينها مع القوانين المحلية بما في ذلك، على سبيل المثال لا الحصر، لوائح الخصوصية، مثل General Data Protection Regulation (GDPR) و EC (ePrivacy) Directive/58/2002 أو ما يعادلها في الإقليم ذي الصلة.
- ب) يجب ألا تقوم مكونات الطرف الثالث المدمجة (مثل المكتبات) بجمع بيانات المستخدم و/أو معالجتها و/أو تخزينها.

² إصدارات المنتج التي يتم دعمها بشكل نشط وفعال وتخضع لتحديثات أمان وصيانة منتظمة من مالك المنصة أو المورد.

- 10-** يجب ألا تجعل تطبيقات الأجهزة المحمولة بيانات التطبيق ممكن الوصول إليها عالميًا.
- أ)** إذا كانت مشاركة البيانات مع التطبيقات الأخرى مطلوبة، يجب أن تستخدم التطبيقات التقنيات والأساليب والضوابط المعقولة تجاريًا لأنظمة التشغيل ذات الصلة لمشاركة القدر الضروري فقط من البيانات مع الحد الأدنى من التطبيقات الأخرى حيث تكون مشاركة البيانات هذه مبررة وموثقة بشكل صحيح.
- 11-** يجب أن تعتمد تطبيقات الأجهزة المحمولة فقط على مرافق الاتصال الآمن التي توفرها أنظمة تشغيل الأجهزة المحمولة ذات الصلة. على سبيل المثال:
- أ)** يجب أن تصرح تطبيقات Android صراحةً أن حركة مرور البيانات غير الآمنة على الشبكة غير مسموح بها تجاه أي نطاق شبكة في بيان التطبيق و/أو ملف تكوين الشبكة الخاص بالتطبيق.
- ب)** يجب أن تستخدم تطبيقات iOS/iPadOS أمان نقل التطبيقات (ATS) دون أي استثناء.
- 12-** يجب ربط مواد التشفير بمخزن مفاتيح آمن مدعوم بالأجهزة.
- 13-** يجب أن تكون تطبيقات الهاتف المحمول مبنية في وضع الإصدار ويجب ألا تحتوي على:
- أ)** أي ميزة أو طريقة يمكن أن تتجاوز ضوابط التحكم،
- ب)** معلومات التصحيح، مثل أسماء ملفات التعليمات البرمجية المصدرية، وأسماء المتغيرات، وأسماء الرموز، والتعليقات، وما إلى ذلك من المعلومات التي يحتمل أن تسهل الهندسة العكسية.
- 14-** يجب أن تكون تطبيقات الهاتف المحمول مزودة بآليات فعالة لمكافحة الاختراق أو التلاعب لمنع حقن التعليمات البرمجية الخبيثة التي يمكن أن تغير أو تراقب سلوك التطبيق في وقت التشغيل.
- 15-** يجب أن تطبق تطبيقات الهاتف المحمول تقنيات شاملة لمكافحة تصحيح الأخطاء أو تقنيات مكافحة الهندسة العكسية/التشويش لإعاقة هجمات الهندسة العكسية.
- 16-** يجب أن تكون حزم تطبيقات الهاتف المحمول مزودة بإمكانية تتيج التحقق من صحة وسلامة محتواها (على سبيل المثال، باستخدام المجموع الاختباري المُشفَّر و/أو التوقيع الرقمي).
- 17-** إذا كان تطبيق الهاتف المحمول يتطلب المصادقة على المستخدم، فيجب إكمال عمليات التحقق من سلامة التطبيق و/أو الجهاز قبل بدء عملية المصادقة على المستخدم.
- 18-** يجب أن تعتمد تطبيقات الهاتف المحمول التي يمكنها الوصول إلى/معالجة/تخزين أي معلومات مملوكة لـ Citi والتي تحمل تصنيف Citi سري أو أعلى و/أو التي يكون تصنيف مخاطر أمن المعلومات (IS) فيها متوسط أو أعلى على استخدام طرق بيومترية قوية حصراً (على سبيل المثال، تلبية أو تجاوز الفئة 3/الفئة القوية كما هو محدد في الوثيقة المقابلة على هذا الرابط [Android Compatibility Definition Document](#)).
- 19-** يجب أن تطبق تطبيقات الهاتف المحمول تدابير مضادة للحماية من هجمات الاختراق (MitM).
- 20-** يجب أن تكون تطبيقات الهاتف المحمول قادرة على اكتشاف الأجهزة التي تعرضت للاختراق التي تشمل، على سبيل المثال لا الحصر، الأجهزة المحمولة التي تم خرق حمايتها أو انتهاك قيودها والتفاعل بما يتماشى مع تقييم المخاطر والمتطلبات التنظيمية للشركة.
- 21-** يجب أن تنفذ تطبيقات الهاتف المحمول ربطاً قوياً للأجهزة لمنع استنساخ الرمز المميز للبرامج (مثل إثبات الملكية).
- 22-** يجب أن تستخدم تطبيقات الهاتف المحمول تطبيقات/حلول لوحة المفاتيح الآمنة (مثل، تلك المدمجة/المثبتة مسبقاً في أنظمة تشغيل الهاتف المحمول).
- 23-** يجب ألا تحتوي الإشعارات الفورية على أي معلومات حساسة (مثل معلومات Citi المصنفة على أنها سرية أو عليا). ومع ذلك، يمكن أن يتم توزيع كلمة المرور لمرة واحدة (OTP) عن طريق إشعار فوري.
- 24-** يجب أن تكون حلول تطبيقات الأجهزة المحمولة مزودة بقدرة على رفض/تجاهل محاولات التواصل مع عملاء الأجهزة المحمولة التي تستخدم إصدار (إصدارات) التطبيقات التي تحتوي على ثغرات معروفة/قابلة للاستغلال.
- 25-** يجب أن تلتزم تطبيقات الهاتف المحمول بأفضل الممارسات في المجال، بما في ذلك، على سبيل المثال لا الحصر، تقنيات الوقاية المنشورة في قائمة OWASP لأفضل 10 تطبيقات للهواتف المحمولة [OWASP Mobile Top 10](#).

- 26-** يجب أن تقوم تطبيقات الهاتف المحمول التي تستغل تقنيات الذكاء الاصطناعي وتعلم الآلة (AI/ML) بذلك بشكل أخلاقي ووفقاً للقسم 19 - الذكاء الاصطناعي/تعلم الآلة (بما في ذلك الذكاء الاصطناعي التوليدي/الذكاء الاصطناعي الوكيل).
- 27-** يجب أن يستخدم تطبيق الهاتف المحمول الحد الأدنى من إذن (أذونات) الجهاز المطلوبة لأداء الغرض (الأغراض)/الوظيفة (الوظائف) التي يستخدمها Citi.
- 28-** يحظر أن تقوم تطبيقات الهاتف المحمول بتخزين أي معلومات غير عامة على وحدة تخزين خارجية/قابلية للإزالة، مثل بطاقات SD.

65-17 الإفصاح عن البرامج

يجب على المورد الإفصاح عن أي وجميع مكونات البرامج، بما في ذلك على سبيل المثال لا الحصر، البرامج مفتوحة المصدر المتضمنة في أي منتجات أو خدمات يتم توفيرها إلى Citi (يُشار إليها مجتمعة باسم "مكونات البرامج"). يلتزم المورد بعدم دمج أي مكونات برمجية، عبر أي تحديث أو ترقية أو غير ذلك، في أي إصدار من المنتجات أو الخدمات المراد تثبيتها على أنظمة Citi، دون إبلاغ Citi مسبقاً في كل حالة. فضلاً عن ذلك، يجب على المورد التأكد من أن منتجاته أو خدماته لا تتضمن مكونات برامج مرخصة بموجب أي شروط تُخضع Citi أو الشركات التابعة له لأي التزامات لم يتم الإفصاح عنها صراحةً إلى Citi وقبولها من جانب Citi في اتفاق بهذا الخصوص. يجب على المورد الإفصاح إلى Citi عن أي مكونات برامج ضارة يتم اكتشافها داخل مؤسسة المورد أو منتجاته أو خدماته في غضون 30 يوماً من اكتشافه لها. يجب على المورد تحديداً الإفصاح عن استخدامه لمكونات البرامج في كل إصدار ونسخة من المنتجات أو الخدمات من خلال تزويد Citi بقائمة ("SBOM") Software Bill of Materials سواء بتنسيق ملف OWASP CycloneDX أو بتنسيق ملف مواصفات تبادل بيانات حزمة البرامج ISO/IEC 5962:2021 Software Package Data Exchange ("SPDX"). يجب أن يتضمن ذلك الإفصاح منشأ مكونات البرنامج (مثل المورد التجاري، أو قاعدة البيانات المدمجة، أو مدير حزم البرامج الثنائية العامة، أو المبنية من التعليمات البرمجية المصدرية، أو أي برنامج مدمج، أو موفر مكونات البرامج المنسقة)، وما إذا كان المورد أو أي من تابعي المورد في سلسلة توريد البرمجيات قد أخذ نسخة من مكونات البرنامج (المعروفة باسم "تنسب البيانات") وقام لاحقاً بدمجها في منتجاته أو خدماته سواء كحزمة تابعة أو كتعليمات برمجية مصدرية مدمجة في التعليمات البرمجية المصدرية للمورد التي يتم تجميع المنتجات والخدمات منها.

66-17 نمذجة التهديدات

يجب على المورد تنفيذ عملية نمذجة التهديدات التي تعالج و/أو تتضمن بشكل شامل كل ما يلي:

- 1-** تعريف النطاق: يجب أن يحدد المورد بوضوح نطاق نموذج التهديد، مع التركيز على مكونات البرامج وتدفقات البيانات التي تعالج معلومات Citi السرية والعليا أو تخزينها أو نقلها.
- 2-** تحديد التهديدات: يجب على المورد أن يحدد بشكل منهجي التهديدات المحتملة والثغرات الأمنية ذات الصلة بتصميم البرنامج وبنيتها واستخدامه المقصود، مع الأخذ في الاعتبار مختلف مسارات الهجوم المختلفة والجهات الفاعلة التي تشكل تهديدات في وقت مبكر من دورة حياة التصميم.
- 3-** تحليل المخاطر: يجب على المورد تحليل التهديدات المحددة لتقييم تأثيرها المحتمل واحتمالية حدوثها، مما يتيح تحديد أولويات المخاطر الأمنية.
- 4-** تكامل الضوابط الأمنية: يجب على المورد تحديد ودمج الضوابط الأمنية واستراتيجيات التخفيف المناسبة في تصميم البرنامج وتطويره لمعالجة هذه المخاطر ذات الأولوية.
- 5-** التوثيق: يجب على المورد توثيق نموذج التهديدات، بما في ذلك التهديدات المحددة والمخاطر المرتبطة وتدابير التخفيف المقابلة التي يتم تنفيذها.
- 6-** المراجعة الدورية: يجب على المورد مراجعة وتحديث نماذج التهديدات بشكل منتظم، ولا سيما عندما تكون هناك تغييرات كبيرة في تصميم البرنامج أو وظائفه أو بيئة نشره.

67-17 الذكاء الاصطناعي

- 1-** يجب على الموردين تنفيذ دورة حياة أمانة لتطوير البرمجيات (SSDLC) تتسم بالقوة والالتزام بها لجميع أنظمة ومكونات AI/ML المقدمة إلى Citi أو المدمجة مع Citi. ويشمل ذلك التصميم والتطوير والاختبار والنشر والصيانة المستمرة بشكل آمن.

- 2- يجب أن تُظهر أنظمة الذكاء الاصطناعي التي يوفرها الموردون نزاهة في عملياتها ومقاومة قوية للهجمات المعادية. ويشمل ذلك تنفيذ آليات للكشف الفوري عن الحقن، وتنظيف المدخلات، والحفاظ على عزل البيانات.
 - 3- يجب أن تتفاعل عوامل ومكونات الذكاء الاصطناعي التي يقدمها الموردون مع أنظمة Citi والأدوات الأخرى بشكل آمن. ويتطلب ذلك إدارة قوية للهوية والوصول، والتحقق الصارم من صحة معاملات تنفيذ الأدوات، وعزل عمليات الأدوات عالية المخاطر. يجب دمج آليات التدخل البشري (HITL) في الإجراءات الحساسة أو عالية المخاطر.
 - 4- يجب أن تُنشئ أنظمة الذكاء الاصطناعي الخاصة بالموردين سجلات شاملة وغير قابلة للتغيير وقابلة للتدقيق لجميع الأحداث الهامة. ويجب حماية هذه السجلات من التلاعب بها وتجميعها والاحتفاظ بها وفقاً لسياسات Citi. ويلزم توفير قدرات مستمرة للرصد والكشف عن حالات الشذوذ لتحديد الحوادث المتصلة بالأمن والأنشطة المشبوهة والإبلاغ عنها.
 - 5- يجب أن تدعم أنظمة الذكاء الاصطناعي الخاصة بالمورد الإشراف البشري على أساس المخاطر، مما يسمح بالتدخل المناسب، وأن تكون مصممة مع إمكانية مساءلة واضحة لمخرجات وإجراءات الذكاء الاصطناعي. ويشمل هذا تصنيف مخرجات الذكاء الاصطناعي حسب مستوى المخاطر ودعم قدرات التدخل البشري.
 - 6- يجب أن يُطبق جميع وكلاء ومكونات وأنظمة الذكاء الاصطناعي التي يقدمها الموردون ضوابط قوية لإدارة الهوية والوصول. يجب أن يُعزى كل تفاعل مع الذكاء الاصطناعي إلى هوية يمكن تحديدها (بشرية أو غير بشرية)، مع ضرورة المصادقة لجميع عمليات الوصول. يجب على وكلاء الذكاء الاصطناعي استخدام الهويات المُدارة واتباع مبادئ الحد الأدنى من الامتيازات عند الوصول إلى موارد Citi.
- (أ) يجب على الموردين توفير وضمان تكليف جميع وكلاء الذكاء الاصطناعي بهويات وكيل Citi Identity and Access (COIN)، الموحدة مع أنظمة Citi Management (IAM) لدى Citi، لتمكين تطبيق سياسات الأمان وإدارة الهوية المركزية وقابلية التدقيق.
- (ب) يجب على الموردين إعداد وكلاء تابعين لجهات خارجية لعملية COIN باستخدام آليات التكامل المعتمدة من Citi، بما في ذلك COIN API المتاحة عبر بوابات أمانة (مثل بوابة SSG Gateway أو Apigee)، ويجب عليهم التأكد من تنفيذ عملية الإعداد هذه بطريقة آمنة وفقاً لمتطلبات الأمان المعمول بها لدى Citi.
- (ج) يجب على الموردين، في حالة استضافتهم داخلياً، إنشاء رمزهم المميز الذي يتوافق مع COIN؛ أما الموردون الذين يستضيفون خدماتهم خارجياً ويستخدمون رمزهم المميز الخاص للتحقق من الهوية الواردة، فيجب أن يكون لديهم رمز تبادل مدعوم لرموز Citi، مثل التبادل من MSFT إلى رموز COIN. يجب مراجعة أي نوع رمز جديد غير مدعوم حالياً من خلال التبادل لاعتماده من قبل فريق IAM في Citi.
- 7- عندما يستخدم الموردون أو يقدمون خوادم أو عملاء Model Context Protocol (MCP)، يجب عليهم تنفيذ MCP RFC 7591 بما في ذلك جميع الميزات الاختيارية.
 - 8- يجب على أنظمة الذكاء الاصطناعي الخاصة بالمورد توفير الحماية لمطالبات النظام وعملياته الداخلية من الكشف أو التلاعب. يجب على إدارة السياق فرض حدود صارمة لمنع تسرب البيانات بين المستأجرين أو المستخدمين أو البيئات.
 - 9- يجب أن يكون لدى الموردين إجراءات موثقة للكشف عن الحوادث الأمنية الخاصة بالذكاء الاصطناعي والاستجابة لها والإبلاغ عنها، بما في ذلك الهجمات العدائية أو التلاعب بالنموذج أو إجراءات الذكاء الاصطناعي غير المصرح بها أو خروقات البيانات التي تنطوي على أنظمة الذكاء الاصطناعي. يجب إخطار Citi على الفور بأي حوادث من هذا القبيل.

18 المبادئ التوجيهية لمكان العمل الآمن

تسري على الموردين 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 يطلبون وصول دون مرافقة إلى مرافق Citi.

يجب على الموردين الحفاظ على الأصول المادية وغير المادية المملوكة لدى Citi وعملائه. ولا يجوز استخدام أصول Citi والعملاء إلا للأغراض المعتمدة وبالطرق المعتمدة (على سبيل المثال، وفقاً للتراخيص والشروط والأحكام المعمول بها)، ثم فيما يتعلق فقط بالأغراض التجارية لدى Citi ومورديه. وتشمل الأصول النقد والأوراق المالية والممتلكات المادية والخدمات

وخطط الأعمال والمعلومات التي تخص Citi ومعلومات الموردين ومعلومات الموزعين والملكية الفكرية (برامج الحاسوب والنماذج والعناصر الأخرى) وجميع المعلومات الشخصية ومسجلة الملكية والمعلومات السرية الأخرى. يُعتبر اختلاس أصول Citi أو الإفصاح غير المصرح به عنها انتهاكاً لواجبك تجاهه وقد يشكل نوعاً من أعمال الاحتيال ضد Citi. وبالمثل، فإن الإهمال أو الهدر أو الاستخدام غير المصرح به لأصول Citi يمثل أيضاً انتهاكاً لواجبك تجاه Citi.

العنصر	المتطلبات
معلومات Citi (الوثائق الإلكترونية والورقية)	قفل معلومات Citi وتأمينها بعد ساعات العمل العادية وفي أي وقت يكون فيه المورد 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 المورد مكان العمل المخصص، يجب عليه قفل الحاسوب الشخصي و/أو الحاسوب المحمول من خلال الضغط على CTRL + ALT + DEL ثم اختيار Lock Computer "قفل الكمبيوتر". إذا كان المورد 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 خصيصاً لهذا الغرض وتوثيقها لدى Citi.
الطابعات وآلات النسخ الفوتوغرافي وأجهزة الفاكس	يجب إزالة جميع المواد التي تخص 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 محددة للاحتفاظ). ويجب تمزيق الوثائق تماماً أو وضعها في سلة محذوفات آمنة/مقفلة. ويجب التخلص من الوسائط المغناطيسية بشكل آمن بعد اتباع إجراءات المسح المناسبة.

19 الذكاء الاصطناعي/تعلم الآلة (بما في ذلك الذكاء الاصطناعي التوليدي/الذكاء الاصطناعي الوكيل)

ينطبق على الموردين الذين يستخدمون الذكاء الاصطناعي/تعلم الآلة (AI/ML)، بما في ذلك الذكاء الاصطناعي التوليدي/الذكاء الاصطناعي الوكيل على النحو المحدد من قبل Citi في هذه المتطلبات الخاصة بالموردين، في أي جزء من المنتج/الخدمة التي يقدمونها.

1-19 يحظر على المورد استخدام تقنيات الذكاء الاصطناعي/تعلم الآلة (AI/ML) الموصوف أدناه، وضمان عدم استخدام أي مقاولين من الباطن له، ما لم يتم الاتفاق على ذلك الاستخدام بين الطرفين في الجدول أو أمر العمل المعمول به بموجب العقد، وذلك في أي من الحالات التالية:

ج) إذا كانت مستخدمة أو مضمنة أو مدمجة بأي شكل من الأشكال في أي منتجات أو خدمات بموجب العقد لتقديمها بشكل مباشر أو غير مباشر إلى Citi، أو في أي جزء منها، بما في ذلك أي منتجات أو خدمات لأطراف ثالثة متضمنة أو مدمجة فيها؛ أو

- 2- إذا استخدمت بأي شكل في تنفيذ المورد لأي عقد، بغض النظر عن استخدام الذكاء الاصطناعي/تعلم الآلة أو تضمينها أو دمجها بطريقة أخرى في المنتج أو الخدمة الفعلية التي يتم تقديمها إلى Citi أو عدم استخدامها؛ أو
- 3- إذا استخدمها المورد بأي طريقة قد تعرض معلومات Citi إلى ذلك الذكاء الاصطناعي/التعلم الآلي (AI/ML)، بما في ذلك، على سبيل المثال لا الحصر، أي AI/ML يستخدمه المورد في عمليات أعماله غير التجارية (مثل حفظ سجلات الأعمال وتحسين العمليات والبحوث والتطوير والامتثال والتدقيق الداخلي).

2-19 يعتبر فشل المورد في الامتثال لهذه الالتزامات خرقاً جوهرياً لشروط هذه الاتفاقية.

3-19 إذا طلبت جهة تنظيمية ذلك، كجزء من أي عملية فحص تنظيمي أو تحقيق جنائي في استخدام AI/ML في أي جزء من المنتج/الخدمة، يجب على المورد 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 تشكل نماذج AI/ML.

4-19 يجب أيضاً الالتزام بالمبادئ التالية:

الشرعية. سوف يتوافق الذكاء الاصطناعي/التعلم الآلي (AI/ML) الخاص بالمورد مع القانون المعمول به.

الغرض والتناسب. لا يحق للمورد دمج المحتوى أو معلومات Citi مع بيانات المورد أو أي طرف ثالث. يحظر على المورد استخدام المحتوى أو معلومات Citi لتدريب AI/ML دون الحصول على موافقة كتابية من Citi. يحظر على الذكاء الاصطناعي/التعلم الآلي (AI/ML) الخاص بالمورد استخدام المحتوى أو معلومات Citi، إلا بالقدر الضروري لتوفير الخدمات.

20 شكاوى العملاء

1-20 الشكاوى عبارة عن مخاطبة شفوية أو كتابية، يمكن استلامها شفهيًا (شخصيًا أو عبر الهاتف) أو كتابيًا (عبر البريد أو عبر الاتصالات الإلكترونية مثل البريد الإلكتروني أو الدردشة أو وسائل التواصل الاجتماعي، وما إلى ذلك)، حيث تعبر عن عدم الرضا من جانب أحد العملاء؛ أو من غير العملاء؛ أو العملاء المحتملين أو عملاء Citi أو المستهلكين المحتملين أو ممثلي العملاء المفوضين (يُشار إليهم مجتمعين باسم "العميل") بخصوص Citi Policy أو أحد المنتجات أو الخدمات التي يقدمها Citi أو التي تُقدم من خلاله، أو موظفي Citi أو مقاولي Citi أو مزودي الخدمات الخارجيين الذين يعملون نيابةً عن Citi أو أي مزيج مما ذكر أعلاه.

2-20 يجب على الموردين الالتزام بسياسة Citi Customer Complaint Handling Policy، بالإضافة إلى أي معايير وإجراءات متعلقة بشكاوى Citi المعمول بها. يخطر المورد جهة الاتصال الرئيسية للأعمال في Citi الخاصة به (أو من ينوب عن جهة الاتصال هذه) كتابيًا في غضون أربع وعشرين (24) ساعة بأي شكاوى كتابية أو شفوية تنطوي على عدم الرضا أو القلق (يُشار إلى كل منها باسم "شكاوى") يتلقاها المورد من أي عميل (أو من غير العملاء الحاليين أو العملاء المحتملين، وفقًا لتعريف الشكاوى لدى Citi) أو من أي جهة تنظيمية ذات صلة فيما يتعلق بالخدمات التي يقدمها المورد نيابةً عن Citi أو فيما يخص Citi بأي شكل من الأشكال. ما لم يوفر Citi ذلك النظام للمورد، فسوف يقوم المورد أيضًا بتطوير وتنفيذ وصيانة نظام (يُشار إليه باسم "نظام التتبع") بما يحقق رضا Citi بشكل معقول لتتبع الشكاوى وتزويد Citi، وفقًا لتقديره، بنسخة من التقارير أو بإمكانية الوصول إلى النظام. يقوم نظام التتبع بالوظائف الآتية:

- أ) تصنيف الشكاوى حسب النوع وتاريخ الاستلام وتاريخ تقديم إشعار الشكاوى إلى Citi،
- ب) وتتبع مسار التعامل مع الشكاوى حتى الانتهاء/حلها،
- ج) وتوفير جميع الأمور الأخرى التي قد يطلبها Citi بشكل معقول. ويجب تصميم نظام التتبع بما يسمح للمورد بتحديد ما إذا كان يتلقى عددًا هائلًا من الشكاوى فيما يتعلق بمسألة معينة حتى يتمكن المورد (بالتشاور مع Citi)

من تحديد ما إذا كانت هناك مشكلة منهجية تتعلق بأعمال المورد أو تقديمه للخدمات وليتمكن على الفور من تصحيح المشاكل.

21 سياسة التداول الشخصي والاستثمار

تحدد سياسة (PTIP) Citi's Personal Trading and Investment Policy، المعنية بالتداول الشخصي والاستثمار، أنشطة التداول والاستثمار المسموح بها والمحظورة، ومتطلبات الموافقة المسبقة، والمتطلبات المتعلقة بالصيانة والإفصاح ومراقبة حسابات الوساطة أو التداول الخاصة بالشخص المشمول بالتغطية. وهي تضع الحد الأدنى من المعايير لتعزيز الامتثال للقوانين واللوائح لمنع الاستخدام غير المشروع للمنصب الوظيفي للفرد لدى Citi أو علاقته مع Citi بما في ذلك معرفة الفرد بشأن (1) المعلومات الجوهرية غير المعلنة أو معلومات المصادر المطلعة (يشار إليها مجتمعة باسم "MNPI") فيما يخص Citi أو طرف ثالث؛ أو (2) المعلومات التي تتعلق بمراكز ومعاملات واستراتيجيات الأوراق المالية والمشتقات والسلع الخاصة بالعملاء.

يجب على جميع موظفي الموردين الذين يحتاجون إلى الوصول المنتظم إلى MNPI كجزء من مسؤولياتهم الوظيفية في Citi والمصنفين كأشخاص مشمولين بالتغطية و/أو أفراد Citi Access الالتزام بالمتطلبات الواردة في PTIP. يجب على موظفي المورد الامتثال للطلبات الواردة من ICRM المتعلقة بالإفصاح عن الحسابات الشخصية، والموافقة المسبقة على أنشطة التداول الشخصي، والقيود المفروضة على التداول الشخصي وتقديم الكشوف والقوائم الدورية.

22 معايير الفوترة والفواتير

فيما يتصل بجهود Citi لتحسين ملاءمة الخدمة زمنياً وتعزيز الضوابط، يتعين على جميع الموردين دعم طرق تقديم الفواتير المفضلة لدى Citi، بالإضافة إلى الخيارات المفضلة لدفع الفواتير، كما هو مفصل أدناه:

- سيقوم المورد بإنشاء ملفات إلكترونية يتم إرسالها إلى Citi بالتنسيق الذي أبلغ به Citi المورد و/أو يقوم المورد باستخدام أداة Citi iSupplier لإدخال بيانات الفاتورة/الفوترة المطلوبة لنقلها رقمياً إلى Citi في وقت لاحق.
- وسوف يقوم المورد بتزويد Citi بجميع المعلومات المصرفية والوثائق الداعمة المطلوبة لتفسير الدفع الإلكتروني للمورد و/أو الاستفادة من عرض Citi لإنجاز المدفوعات باستخدام البطاقة الافتراضية (طالما كانت متوفرة).

ملاحظة: يتم احتساب شروط الدفع بدءاً من تاريخ استلام Citi لطلب الفاتورة.

للدفع في الوقت المناسب والوفاء بالالتزامات التعاقدية، يطلب Citi من جميع الموردين تضمين بيانات الفاتورة التالية والالتزام بالمبادئ التوجيهية المرتبطة عند إرسال فواتير إلى Citi مقابل السلع أو الخدمات:

- 1- كيان الأعمال الصحيح في Citi، وعنوان الجهة التي يتم توجيه الفاتورة إليها "Bill to"، واسم جهة الاتصال التجارية المرتبطة بـ Citi.
- 2- رقم الفاتورة، وتاريخ الفاتورة، ورقم أمر الشراء.
- 3- يتم إرسال الفواتير إلى مقر Citi أو عنوان البريد الإلكتروني المفصل في طلب شراء Citi.
- 4- يجب أن تتضمن السلع أو الخدمات التي يتم إصدار فواتير بشأنها تفاصيل واضحة ووصفية داخل الفاتورة.
- 5- لا يتم إدراج شيء سوى الرسوم الحالية الخاصة بالفاتورة المحددة (ينبغي عدم إدراج أرصدة الفواتير المعلقة غير المدفوعة الأخرى).
- 6- ويتم إصدار الفواتير باللغة الإنجليزية، بما في ذلك الوثائق الداعمة.

23 سياسة الغياب الإلزامي

تتطلب سياسة الغياب الإلزامي لدى Citi من الأفراد الذين يؤدون أنشطة حساسة أو عالية المخاطر، ولا سيما تلك التي تؤثر على دفاتر وسجلات الشركة، الابتعاد بشكل دوري عن هذه المهام. يهدف هذا الفصل التفسيري إلى تعزيز الضوابط الداخلية

من خلال خلق فرص للكشف عن الاحتيال المحتمل أو السرقة أو أي سوء سلوك آخر قد يظل مخفياً لولا ذلك. وتتوافق السياسة مع التوقعات الإشرافية التي حددها مجلس الاحتياطي الفيدرالي الأمريكي بشأن الغياب الإلزامي للموظفين الذين يشغلون مناصب حساسة.

يجب على جميع موظفي المورد الذين يمكنهم الوصول إلى البيانات الحساسة وكجزء من مسؤولياتهم الوظيفية في Citi والمصنفين بوصفهم أشخاص "يشغلون مناصب حساسة" الالتزام بالمتطلبات المنصوص عليها في MA Policy. يجب على الأشخاص الذين يشغلون مناصب حساسة كل عام تحديد فترة غياب إلزامي وإكمالها بالكامل، مع الالتزام التام بجميع قواعد السياسة وقبورها. خلال هذه الفترة، يجب عليهم عدم تنفيذ أي أنشطة حساسة أو توجيهها أو التصريح بها أو اعتمادها، كما يجب عليهم عدم الرد من أساسه على أي مراسلات - بما في ذلك تفاعلات العملاء - باستثناء إعادة توجيه الاستفسارات بشأن التغطية. في حال الحاجة إلى قطع فترة الغياب بعد بدئها، يجب على المديرين أو جهات الاتصال التجارية في Citi إلغاؤها في أنظمة الامتثال لاستعادة الوصول إلى النظام، وبعد ذلك يتعين على الموظف إعادة جدولة فترة غياب جديدة.

ملحق - 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 منقطة الاتصال من التعرض للهجمات الإلكترونية وتسمح باستعادة البيانات إلى ما كانت عليه قبل بدء الهجوم.

يشمل **القانون المعمول به:** (أ) القوانين واللوائح الصادرة عن الولاية 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. ويشمل هذا جميع فئات الذكاء الاصطناعي (AI) الموضحة أدناه، بالإضافة إلى تغييرات الذكاء الاصطناعي (AI) - على سبيل المثال: الذكاء الاصطناعي التوليدي (Gen AI)، والذكاء الاصطناعي الوكيل، ونماذج اللغة الكبيرة، ونماذج الذكاء الاصطناعي للأغراض العامة (GPAI) وما إلى ذلك.

تشمل فئات الذكاء الاصطناعي ما يلي:

- **الذكاء الاصطناعي الثابت:** هو تقنيات الذكاء الاصطناعي التي يتم تدريبها يدويًا دون الاتصال بالإنترنت أو التي تتم برمجة معلوماتها بشكل صريح ثم استخدامها بعد ذلك لإجراء تقديرات أو تنبؤات أو وضع توصيات أو صنع قرارات.
- **الذكاء الاصطناعي الديناميكي:** هو التقنيات التي يمكنها تلقائيًا إعادة تدريب المعلومات بشكل دوري في الإنتاج، وذلك على عكس "الذكاء الاصطناعي الثابت".
- **الذكاء الاصطناعي الآلي:** هو تقنيات "الذكاء الاصطناعي الديناميكي" التي يمكنها بالإضافة إلى ذلك تغيير هيكلها الأساسي تلقائيًا (مثل المعلومات 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.

التعلم الآلي هو مجموعة فرعية من الذكاء الاصطناعي تعتمد 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): هو أحد موظفي Citi يقع على عاتقه مسؤولية تنفيذ أنشطة معينة مقترنة بعلاقات المورد وإدارتها بنشاط.

مقدم الأعمال هو مورد يُستخدم من قبل Citi للعمل نيابةً عن Citi لتحديد فرص الأعمال الجديدة أو إدارة علاقات العملاء الموجودة بالفعل.

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

معلومات Citi: هي المعلومات التي يمتلكها Citi أو يلتزم بحمايتها أثناء مرحلة التخزين أو النقل أو التخلص منها سواء بالتنسيقات الرقمية أو غير الرقمية.

تشمل تصنيفات معلومات Citi:

السرية - والمعلومات السرية هي المعلومات المتعلقة بأعمال Citi و/أو الأطراف ذات الصلة التي لا تشير إلى الأفراد وتتطلب مستوى عالٍ من الحماية. ويكون لانتهاك سرية هذه المعلومات أو سلامتها أو توافرها تأثير خطير على عمليات Citi أو وضعه المالي أو امتيازته أو عملائه من الشركات.

معلومات تحديد الهوية الشخصية السرية هي معلومات شخصية عن فرد ما يمكن أن تسهل نشاطاً غير قانوني مثل سرقة الهوية أو الاحتيال الائتماني أو أي احتيال مالي آخر ضد الفرد المذكور. ويكون لانتهاك سرية هذه المعلومات أو سلامتها أو توافرها تأثير كبير على الفرد (الأفراد)، بما في ذلك، على سبيل المثال لا الحصر، الخسارة المالية أو الاحتيال.

○ وعند دمج عناصر البيانات الشخصية مع بيانات شخصية أخرى، فإنها تشكل PII سرية، وتشمل اسم الفرد أو معلومات الاتصال (العنوان، أو رقم الهاتف، أو عنوان البريد الإلكتروني) بالإضافة إلى:

- عناصر بيانات المعاملات التي قد يترتب عليها حركة الأموال، أو التي يمكن استخدامها لارتكاب سرقة الهوية أو الاحتيال، مثل:
- رقم بطاقة الائتمان/الخصم المباشر.
- قيمة التحقق من البطاقة (CVV) أو PIN
- بيانات التقرير الائتماني (درجة الائتمان)
- تاريخ الميلاد بالكامل
- أداء العامل (التقييم/الملاحظات)، أو معلومات التعويضات
- تسجيلات الفيديو، وتشمل CCTV وسجلات ATM

● تشكل بعض عناصر البيانات الشخصية بمعزل عن غيرها معلومات تحديد هوية شخصية سرية:

○ رقم الضمان الاجتماعي الأمريكي، أو رقم إثبات هوية صادرة عن الحكومة (والذي يعادل في استخدامه و/أو حالة الحماية القانونية رقم الضمان الاجتماعي الأمريكي) أو رقم جواز السفر أو رقم رخصة القيادة أو رقم الهوية الضريبية للفرد

الداخلية - هي معلومات لا تتعلق بفرد، وليست مخصصة لأغراض تجارية وتتطلب مستوى متوسط من الحماية. ويكون لانتهاك سرية هذه المعلومات أو سلامتها أو توافرها تأثير محدود على الفريق أو مجموعة العمل.

- **معلومات التعريف الشخصية (PII)** هي المعلومات الشخصية والتي تكون أي معلومات:
- تحدد هوية الفرد أو الأسرة أو يمكن استخدامها لتحديد هوية أيًا منهما (مثل الاسم أو التوقيع أو العنوان أو المَعْرِف 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 PIN أو رقم التعريف أو إجابات 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).

العامّة - هي المعلومات المتاحة خارج Citi دون قيود أو التي يُقصد منها استخدامها استخدامًا عامًا، مثل بيانات Citi الصحفية أو المقالات التي يتم عرضها في الأخبار بشأن Citi.

المقيدة هي معلومات محدودة يقتصر استخدامها على أشخاص أو مجموعات محددة وتكون أكثر حساسية بالنسبة إلى Citi أو الشركات التابعة له وتتطلب أعلى مستوى من الحماية. ويكون لانتهاك سرية هذه المعلومات أو سلامتها أو توافرها تأثير خطير (على مستوى المؤسسة أو على مستوى مناطق متعددة أو على مستوى قطاعات متعددة) على عمليات Citi أو وضعه المالي أو امتيازته أو عملائه من الشركات.

○ **Sensitive PII** هي المعلومات الشخصية التي تستدعيها قوانين محددة باعتبارها تحتاج إلى حماية إضافية، ويمكن استخدامها للتمييز غير القانوني ضد فرد ما أو التسبب في ظلمه أو إلحاق الضرر به. ويكون لانتهاك سرية هذه المعلومات أو سلامتها أو توافرها تأثير كبير على الفرد (بما في ذلك، على سبيل المثال لا الحصر، الخسارة المالية أو الاحتيال أو التأثير التمييزي).

■ البيانات المتعلقة خصيصًا بكل 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 بالميراث أو الأنشطة الجنسية الخاصة بالفرد.

○ المعلومات الصحية الشخصية (PHI) التي تتضمن معلومات بشأن السجل الطبي أو الحالة العقلية أو البدنية للفرد.

العميل يعني أي عميل أو زبون لدى 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.

معدات وأنظمة وخدمات الاتصالات: هي أي أجهزة أو برامج أو تطبيقات تُستخدم في نقل الاتصالات الإلكترونية المكتوبة أو الصوتية أو المرئية؛ وتشمل 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 الإنترنت 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 التي تخص Citi وأي بيانات أو تقارير أو إحصائيات أو معلومات أخرى من أي نوع (أ) تم تقديمها أو إنتاجها بشكل مباشر أو غير مباشر للمورد من قبل Citi أو نيابة عنه أو الشركات التابعة له أو نيابة عن عملاء أو زبائن أو مقدمي الخدمات لأي منهم، (ب) أو تم إنشاؤها أو إنتاجها عبر الخدمات، (ج) أو تم اشتقاقها 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 لدى Citi وأحد الموردتين. كما تعتبر اتفاقية عدم الإفصاح (NDA) عقدًا لأغراض هذه المعايير.

اختبار حجب الوصول (DOA) يتحقق من مستوى التوظيف والدعم لدى المورد لعمليات أعمال Citi التي يمكن استردادها ضمن RTO المحدد.

اختبار رفض الخدمة (DOS) يتحقق من إمكانية استرداد تطبيق المورد ومكونات البنية التحتية الأساسية التي تدعم أعمال Citi ضمن RTO المحدد.

"مواد الإيداع" تعني الفقرات الفرعية التالية (1) - (6)، مجتمعة، فيما يتعلق، حسب الاقتضاء، بالبرمجيات المرخصة لدى Citi للتشغيل ضمن بيئة Citi أو المواد التي يستخدمها المورد في إنجاز الخدمات المستضافة المقدمة إلى Citi:

(1) نسخة طبق الأصل مكررة من التعليمات البرمجية المصدرية للبرنامج المستخدم في تطوير وتشغيل وصيانة ودعم البرنامج المرخص أو الخدمات المستضافة المنصوص عليها في الاتفاقية المعمول بها مع Citi (وكل الإصدارات اللاحقة من ذلك البرنامج أو من تلك الخدمات المستضافة)، وجميع الوثائق الخاصة بذلك البرنامج (بغض النظر عما إذا كان لدى Citi بالفعل نسخة من أجزاء من تلك التعليمات البرمجية المصدرية) ("إيداع التعليمات البرمجية المصدرية")؛

(2) التعليمات البرمجية المصدرية لأي برنامج تابع لجهة خارجية يتمتع المورد بحقوق فيها فيما يتعلق بتطوير وتشغيل وصيانة ودعم البرنامج المرخص أو الخدمات المستضافة؛

(3) نسخة مرخصة من جميع أدوات البرنامج، مثل أدوات تصحيح الأخطاء والمجمعات والمترجمات اللازمة لتحويل التعليمات البرمجية المصدرية المضمنة في مواد الإيداع إلى نموذج قابل للتنفيذ حسب الضرورة لتشغيل وصيانة ودعم البرنامج أو الخدمات المستضافة؛

(4) إلى الحد الذي لم يتم تقديمه بالفعل أعلاه، أي وثيقة توفر ما يلي: (أ) الأوصاف والعمليات العامة الخاصة بمواد الإيداع؛ (ب) والبنية المعمارية ووظائف البرنامج الأساسية؛ (ج) ومعلومات تدفق البيانات؛ (د) خريطة وقوائم الذاكرة التفصيلية؛ (هـ) وخرائط منافذ الإدخال/الإخراج؛ (و) وأي تفاصيل أخرى تسمح للمبرمج ذي المهارة العادية في لغة (لغات) البرمجة المعمول بها باستخدام وتعديل التعليمات البرمجية المصدرية المضمنة في مواد الإيداع؛

- (5) وجميع المعلومات التقنية الأخرى المتعلقة بالبرنامج أو الخدمات المستضافة والتي قد تكون ضرورية بشكل معقول لتمكين Citi، أو طرف ثالث مختص نيابة عن Citi، من استخدام وتشغيل وتعديل وتحسين البرنامج أو الخدمات؛
- (6) وقائمة بجميع برامج وتقنيات الطرف الثالث المستخدمة فيما يتعلق بالبرنامج أو الخدمات المستضافة، بما في ذلك التفاصيل المعقولة التي تتعلق باستخدامها في البرنامج ومعلومات الاتصال لموفر ذلك البرنامج أو تلك التكنولوجيا. يقر Citi ويوافق على عدم احتواء مواد الإبداع على أي تعليمات برمجية مصدرية من أطراف ثالثة بخلاف ما هو منصوص عليه في الفقرة الفرعية (2)؛ و
- (7) فيما يتعلق بالخدمات المستضافة:

أ) نسخة مصغرة من بيئة الإنتاج المستضافة على السحابة أو المواد المتعلقة بالسحابة الخاصة بالبيئة وغيرها من المعلومات المطلوبة لاستنساخ بيئة إنتاج Citi بما في ذلك (على سبيل المثال لا الحصر): البنية التحتية مثل التعليمات البرمجية ونصوص Terraform، وموارد السحابة، وقوالب تكوين السحابة، وملفات التكوين، ومستأجري السحابة، واشتراكات السحابة، وصور الأجهزة، وصور Docker والبنية التحتية مثل الكود المصدري للبرنامج؛ و

ب) نسخة من بيانات Citi المخزنة داخل البرنامج.

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 النظم إلى نظير أو الرسائل الفورية، ومنشورات المدونات ومنشورات وسائل التواصل الاجتماعي، والرسائل التي يتم إرسالها عبر تطبيقات المراسلات مثل WhatsApp و WeChat و Line و Signal و Viber، 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.

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

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

الاحتياط: 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 المورد 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.

بيانات التحقق من الهوية (IVD) تعرّف بأنها أسئلة الأمان (SQ) أو أسئلة المصادقة القائمة على المعرفة (KBA). وعادةً ما يتم تحديد أسئلة الأمان من قبل التطبيق ويتم الإجابة عليها من قبل المستخدم النهائي. ومن الأمثلة على ذلك اسم الأم قبل الزواج، ومحل الميلاد، والآيس كريم المفضل لديك، وما إلى ذلك. ويجب التعامل مع كلا النوعين من الأسئلة كبيانات للمصادقة.

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 معالجتها 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 باستمرار الأعمال.

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

البرمجيات مفتوحة المصدر تعني رمز المصدر أو برنامج كمبيوتر مجمع يكون فيه رمز المصدر متاحًا لعامة الناس لاستخدامه أو تعديله عن تصميمه الأصلي.

الموظفون: يُقصد بهذا المصطلح، سواء ذكر مباشرة أو مستمداً من السياق، المورد والشركات التابعة له، ومديره ومسؤوليه وموظفيه ووكلائه ومدققي حساباته ومستشاريه ومقدمي خدماتهم ومقاوليه (مع استبعاد موظفي Citi). كما يشمل موظفو المورد أيضاً مديري أي مقاول من الباطن ومسؤوليه وموظفيه ووكلائه ومدققيه ومستشاريه أو أي ممثلين آخرين لأي مقاول من الباطن.

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 بالمعلومات هو مطلب يتم فرضه على السجلات والمعلومات يقضي بإيقاف إدخال أي تعديل عليها أو التخلص منها حتى يتم رفعه بواسطة السلطة التي أصدرت أمر الاحتفاظ.

قدرة الاسترداد هي حجم منتجات وخدمات المورد أو كميته أو سرعة تقديمها معبراً عنه كنسبة مئوية للتسليم العادي للمنتجات والخدمات.

مدة الاسترداد هي المدة القصوى، معبراً عنها بالأيام التقويمية، التي يكون المورد خلالها قادراً 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.

"حدث الإصدار" يعني واحد أو أكثر مما يلي:

(1) (أ) يصبح المورد مفلساً أو يُقرّ بعدم قدرته على سداد ديونه بشكل عام عند استحقاقها؛ (ب) أو يصبح خاضعاً، بشكل طوعي أو غير طوعي، لأي إجراء بموجب أي قانون محلي أو أجنبي في شأن الإفلاس أو الإعسار عندما لا يتم إيقاف ذلك الإجراء بالكامل في غضون سبعة (7) أيام عمل أو لم يتم رفضه أو إلغاؤه في غضون خمسة وأربعين (45) يوماً بعد التقديم؛ (ج) أو يقوم بالتنازل بشكل عام لصالح الدائنين؛ (د) أو يكون لديه حارس قضائي أو أمين أو وصي أو وكيل مماثل يتم تعيينه بأمر من أي محكمة ذات اختصاص قضائي لتولي مسؤولية أي جزء مادي من ممتلكاته أو أعماله أو بيع ذلك الجزء.

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

مدير التوريد في منظمة إدارة الموارد (RMO) هو موظف في منظمة إدارة الموارد (RMO) يكون مسؤولاً عن التفاوض بشأن الشروط التجارية للعقد والمتطلبات والتسعير، بما في ذلك: طلبات RFPs وغيرها من أنشطة اختيار الموردين وإدارة شروط وأحكام العقد ومتطلبات اعتماد التقييم المالي.

التأثير السلبي الخطير أو الكارثي على الفرد يُقصد به أن 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.

المقاول من الباطن: المقاول من الباطن هو طرف رابع (شخص أو كيان)، تم تعيينه من قبل طرف ثالث لأداء بعض أو كل الخدمات أو الأنشطة التي تعاقدها Citi بشأنها مع الطرف الثالث.

التوجيهات:

س1: هل يجب الإبلاغ عن جميع المقاولين من الباطن التابعين لطرف ثالث؟

ج1: يجب الإبلاغ فقط عن المقاولين من الباطن المرتبطين بالخدمة التي يتم تنفيذها. من الأمثلة على الخدمات أو الأنشطة التي يؤديها المقاول من الباطن، على سبيل المثال لا الحصر:

*المقاول من الباطن الذي يؤدي خدمات تقنية أو برمجية تدعم بشكل مباشر أو غير مباشر الخدمة/الأنشطة التي تعاقده Citi مع الطرف الثالث لأدائها؛ أو

*المقاول من الباطن الذي تشمل خدماته الوصول إلى معلومات Citi السرية أو العليا؛ أو

*المقاول من الباطن الذي يكون له تعامل مباشر أو غير مباشر مع أي عميل حالي/محتمل من عملاء Citi؛ أو

*المقاول من الباطن الذي يكون غير مصحوب بمرافق ويقوم بخدمات فرم مستندات Citi أو أرشفتها داخل أو خارج أي مبنى من مباني Citi؛ أو

*المقاول من الباطن الذي يدعم الوظائف أو الخدمات المصرفية الأساسية مثل عمليات الدفع والتحويل والإقراض وما إلى ذلك.

المورد: لأغراض وثيقة متطلبات Citi للموردين "Citi Requirements for Suppliers"، يشير مصطلح "المورد" حصرياً إلى طرف ثالث خارجي دخل في ترتيب تجاري لتوفير المنتجات أو الخدمات مباشرة إلى كيان Citi أو لدعم كيان Citi في تحقيق أهدافه التجارية. يعرف الطرف الثالث الخارجي على أنه كيان غير تابع لدى Citi. ويمكن أن يكون الموردون كذلك عملاء أو زبائن لدى كيان Citi أو يمكن أن يدعموا التفاعلات مع عملاء وزبائن Citi؛ إلا أن الترتيبات التي تعتمد بشكل حصري على كونهم عملاء أو زبائن لدى Citi لا تعد علاقات موردين ضمن نطاق هذه الوثيقة.

المعلومات المؤقتة: السجل هو النسخة النهائية والأكثر اكتمالاً من المعلومات التي يكون Citi ملزماً بالاحتفاظ بها لأسباب قانونية أو تنظيمية أو لأسباب معتمدة ذات صلة بالأعمال. جميع المعلومات الأخرى مصنفة على أنها "معلومات مؤقتة".