

WYMAGANIA CITI DLA DOSTAWCÓW

WŁAŚCICIELE:
Dyrektor Citi Procurement & Risk

DATA WYDANIA:
Styczeń 2015 r.

MODYFIKACJA:
Wrzesień 2026 r.

WERSJA:
9

SPIS TREŚCI

1	OMÓWIENIE	3
2	RÓWNE SZANSE NA ZATRUDNIENIE	5
3	PRZECIWDZIAŁANIE ŁAPOWNICTWU I KORUPCJI (AB&C)	6
4	PREZENTY I ROZRYWKA	7
5	ZAANGAŻOWANIE DOSTAWCÓW I ZASADY DLA DOSTAWCÓW	7
6	ZWALCZANIE WSPÓŁCZESNEGO NIEWOLNICTWA	8
7	PERSONEL DOSTAWCY	10
8	PRZECIWDZIAŁANIE OSZUSTWOM	11
9	KONTAKTY Z MEDIAMI I WYSTĄPIENIA PUBLICZNE	13
10	PISEMNA KOMUNIKACJA ELEKTRONICZNA	14
11	DZIAŁALNOŚĆ POLITYCZNA I FINANSOWANIE KAMPANII	15
12	PRZECIWDZIAŁANIE PRANIU PIENIĘDZY („AML”)	15
13	ZARZĄDZANIE DOKUMENTACJĄ	17
14	ODPORNOŚĆ PRZEDSIĘBIORSTWA / CIĄGŁOŚĆ DZIAŁALNOŚCI BIZNESOWEJ	19
15	GLOBALNE STANDARDY KONTROLI POD KĄTEM NIEKARALNOŚCI	26
16	WYDATKI	28
17	BEZPIECZEŃSTWO INFORMACJI (IS)	29
18	WYTYCZNE DOTYCZĄCE BEZPIECZNEGO MIEJSCA PRACY	70
19	SZTUCZNA INTELIGENCJA / UCZENIE MASZYNOWE (W TYM GENERATYWNA SZTUCZNA INTELIGENCJA / AGENTIC AI)	71
20	SKARGI KLIENTÓW	72
21	POLITYKA DOTYCZĄCA TRANSAKCJI OSOBISTYCH I INWESTYCJI	73
22	STANDARDY ROZLICZEŃ I FAKTUROWANIA	74
23	POLITYKA OBOWIĄZKOWEJ NIEOBECNOŚCI	74
	ZAŁĄCZNIK — DEFINICJE	76

1 OMÓWIENIE

1.1. Wymagania ogólne

Niniejsze Wymagania Citi dla Dostawców („**Wymagania**”) zawierają wyszczególnienie niektórych zobowiązań, które Dostawcy muszą spełnić w trakcie współpracy biznesowej z Citi. Pewne Wymagania mają zastosowanie do wszystkich Dostawców, ale niektóre Wymagania będą odnosić się do konkretnego Dostawcy, zależnie od rodzaju produktów i usług, które Dostawca świadczy na rzecz Citi (te ostatnie podsumowano w Części 1.2 poniżej i wskazano na początku każdego postanowienia wymienionego w niniejszym dokumencie). Terminy pisane wielką literą mają znaczenie przypisane im w niniejszym dokumencie, w tym w dołączonym Załączniku. Jeżeli w niniejszym dokumencie nie wskazano znaczenia danego terminu, wtedy ma on znaczenie przypisane w Umowie, zdefiniowano poniżej.

Niniejsze Wymagania stanowią zobowiązania umowne wynikające z umów Dostawców z Citi (w tym m.in. dokumentów transakcyjnych, np. zleceń pracy, harmonogramów licencji) (każda zwana jest dalej „**Umową**”) i stanowią uzupełnienie wszelkich zobowiązań określonych w Umowie, wszelkich obowiązków wynikających z Obowiązującego prawa (zgodnie z definicją tego terminu poniżej), wszelkich zawiadomień dla Dostawcy od Citi, informujących Dostawcę o jego zobowiązaniach z tego tytułu (każde zwane jest dalej „**Zawiadomieniem**”), lub jakichkolwiek dodatkowych, bardziej szczegółowych wymagań wdrożonych przez jednostki biznesowe lub funkcje Citi. W przypadku sprzeczności pomiędzy powyższymi wymaganiami a ograniczeniami zastosowanie mają bardziej rygorystyczne obowiązki i wymagania. Dostawcy powinni działać proaktywnie i konsultować się ze swoją główną osobą do kontaktu w jednostce biznesowej Citi (lub osobą wyznaczoną) w sprawie pytań dotyczących niniejszych Wymagań, w tym wszelkich ich zmian, wniosków o zwolnienie z ich stosowania lub wszelkich domniemyanych konfliktów z nimi lub z obowiązującym prawem.

Dostawca niezwłocznie zastosuje się do wszelkich uzasadnionych wniosków, które Citi może przesłać Dostawcy w celu uzyskania danych wymaganych przez Citi w związku z Usługami Dostawcy lub Personelem w związku z obowiązkiem Citi dotyczącym przestrzegania obowiązujących przepisów prawa. Nieprzestrzeganie przez Dostawcę tych zobowiązań uznaje się za istotne naruszenie warunków niniejszej Umowy.

Nieprzestrzeganie niniejszych Wymagań lub jakichkolwiek dodatkowych wymogów określonych przez jednostkę biznesową Citi, z którą Dostawca prowadzi interesy, może skutkować rozwiązaniem Umowy Dostawcy z Citi. Ponadto naruszenie Wymagań może również stanowić naruszenie obowiązującego prawa i może skutkować powstaniem odpowiedzialności cywilnej względem Citi (lub stron trzecich) lub sankcjami karnymi dla Dostawcy. Dostawcy nie mogą powoływać się na zgodność z własnymi politykami w zastępie obowiązku przestrzegania postanowień niniejszych Wymagań bez pisemnej zgody Citi.

1.2. Wymagania mające zastosowanie do wybranych Dostawców

W poniższej tabeli przedstawiono konkretne Wymagania mające zastosowanie do niektórych Dostawców, którzy spełniają kryteria stosowności wymienione w niniejszym dokumencie. Części niewymienione poniżej mają zastosowanie do WSZYSTKICH Dostawców.

Nr części	Tytuł części	Zastosowanie
2	RÓWNE SZANSE NA ZATRUDNIENIE / DZIAŁANIA AFIRMATYWNE	Dotyczy umów i zamówień zakupu niezbędnych do zrealizowania postanowień umowy Citi zawartej z rządem federalnym Stanów Zjednoczonych; w przypadku braku pewności, czy umowa lub zamówienie zakupu dotyczą podwykonawstwa, czy zamówienia zakupu rządu federalnego, należy na początku lub końcu klauzuli uwzględnić sformułowanie „Zależnie od przypadku”.
12	PRZECIWDZIAŁANIE PRANIU PIENIĘDZY	Dotyczy Dostawców świadczących konkretne usługi związane z obsługą klientów (na przykład proces wdrażania nowych pracowników, monitorowanie kont klientów i transakcji finansowych) lub dostarczających dane/wskaźniki związane z powyższymi czynnościami; <u>I/LUB</u> Dostawców pełniących funkcję pośrednika w odniesieniu do instrumentów rynku pieniężnego lub finansowych (np. zdalne przyjmowanie depozytów, usługi kurierskie, obsługa samochodów opancerzonych lub skrytek).
13	ZARZĄDZANIE DOKUMENTACJĄ	Dotyczy Dostawców, którzy uzyskują dostęp do Informacji Citi, przetwarzają je lub je przechowują
14	CIĄGŁOŚĆ DZIAŁALNOŚCI BIZNESOWEJ	Dotyczy Dostawców, którzy świadczą usługi lub hostują infrastrukturę technologiczną / aplikacje wykorzystywane przez Citi. Właściciel Działań Biznesowych Citi (BAO) jest odpowiedzialny za przekazanie Dostawcy informacji o możliwości zastosowania i wymaganiach COB.
15	GLOBALNE STANDARDY KONTROLI POD KĄTEM NIEKARALNOŚCI	Dotyczy Dostawców świadczących usługi na rzecz Citi.
16	WYDATKI	Dotyczy Dostawców, którym zgodnie z umową przysługuje prawo do ubiegania się o zwrot kosztów działalności gospodarczej.
17	BEZPIECZEŃSTWO INFORMACJI (IS)	Dotyczy Dostawców, w tym Podwykonawców, którzy uzyskują dostęp do informacji Citi, przetwarzają je, zarządzają nimi lub je przechowują; <u>I/LUB</u> Dostawców odpowiedzialnych jako Host za aplikacje z dostępem do Internetu pod marką Citi; <u>I/LUB</u> Dostawców dysponujących łącznością z zasobami sieciowymi Citi; <u>I/LUB</u> Dostawców mających dostęp do zasobów sieciowych Citi; <u>I/LUB</u> Dostawców wymagających dostępu bez eskorty do pomieszczeń Citi.
18	WYTYCZNE DOTYCZĄCE BEZPIECZNEGO MIEJSCA PRACY	
19	SZTUCZNA INTELIGENCJA / UCZENIE MASZYNOWE (w tym generatywna sztuczna inteligencja / Agentic AI)	Dotyczy Dostawców, którzy wykorzystują sztuczną inteligencję / uczenie maszynowe (AI/ML, Artificial Intelligence / Machine Learning) zgodnie z definicją Citi w dowolnej części produktu lub świadczonej usługi.

Nr części	Tytuł części	Zastosowanie
20	POLITYKA DOTYCZĄCA TRANSAKCJI OSOBISTYCH I INWESTYCJI	Dotyczy Dostawców, którzy wymagają regularnego dostępu do MNPI w ramach swoich obowiązków służbowych w Citi.
23	POLITYKA OBOWIĄZKOWEJ NIEOBECNOŚCI	Niniejsza Polityka ma zastosowanie do Osób niebędących pracownikami („Współpracowników”), które obejmują Stanowiska o podwyższonym ryzyku (zgodnie z definicją w Słowniku) („Współpracownicy na stanowiskach o podwyższonym ryzyku”), a także bezpośrednich kierowników i przełożonych Pracowników na stanowiskach o podwyższonym ryzyku („Kierownicy”), oraz Kontaktów biznesowych Citi tych Pracowników na stanowiskach o podwyższonym ryzyku.

2 RÓWNE SZANSE NA ZATRUDNIENIE

2.1 Równe możliwości zatrudnienia.

Firma Citi opracowała polityki równych szans w zatrudnieniu, które mają na celu zapewnienie równych szans zatrudnienia wszystkim wykwalifikowanym osobom bez względu na rasę, kolor skóry, wyznanie, płeć, orientację seksualną, tożsamość płciową, pochodzenie narodowościowe, obywatelstwo, status imigranta, wiek, stan cywilny, dane genetyczne, niepełnosprawność, status weterana chronionego lub jakąkolwiek inną cechę chronioną przez prawo.

Dostawcy oraz ich personel są zobowiązani do przestrzegania wszelkich obowiązujących przepisów ustawowych i wykonawczych dotyczących niedyskryminacji, w tym m.in. wszelkich takich przepisów ustawowych i wykonawczych, o konieczności przestrzegania których firma Citi powiadomi Dostawcę na piśmie.

Dostawcy będą weryfikować i podejmować odpowiednie działania zgodne z Oświadczeniem Citi dotyczącym polityki równych szans zatrudnienia w Stanach Zjednoczonych, które można znaleźć pod adresem www.citigroup.com/global/eoo-aa-policy.

2.2 Umowy z organami rządowymi

Umowy i zlecenia zakupu, które są niezbędne do zrealizowania postanowień umowy Citi zawartej z rządem federalnym, muszą zawierać następujące, pokazane niżej pogrubione klauzule słowne. (W przypadku braku pewności, czy zlecenie rządu federalnego dotyczy podwykonawstwa, czy zakupu, należy na wszelki wypadek dodać na początku klauzuli sformułowanie „Zależnie od przypadku”).

[Zależnie od przypadku] Dostawca będzie przestrzegać wszystkich obowiązujących federalnych przepisów antydyskryminacyjnych i poświadczają, że nie prowadzi żadnych programów z naruszeniem obowiązujących federalnych przepisów antydyskryminacyjnych.

2.3 Załącznik do umów z organami rządowymi

Umowy i zlecenia zakupu, które są niezbędne do zrealizowania postanowień umowy Citi zawartej z rządem federalnym, muszą zawierać następującą informację w załączniku zlecenia podwykonawstwa lub zakupu. (W przypadku braku pewności, czy zlecenie rządu federalnego dotyczy podwykonawstwa, czy zakupu, na wszelki wypadek należy dodać na końcu zawiadomienia sformułowanie „Zależnie od przypadku”).

Citigroup, jako podwykonawca z sektora federalnego, niniejszym przekazuje niżej podpisanemu podwykonawcy lub dostawcy pisemne powiadomienie o naszych zobowiązaniach do zapewnienia równych szans w zatrudnieniu w imieniu weteranów chronionych i osób niepełnosprawnych. Citigroup działa w pełni zgodnie z sekcją 503 Ustawy o Rehabilitacji (Rehabilitation Act) i Ustawy o pomocy adaptacyjnej dla weteranów konfliktu w Wietnamie (Vietnam Era Veterans' Readjustment Assistance Act), a także z obowiązującymi przepisami – odpowiednio 41 C.F.R. § 60-741 oraz 41 C.F.R. § 60-300. Nasze Oświadczenie dotyczące polityki równych szans zatrudnienia można znaleźć pod adresem www.citigroup.com/global/eeo-aa-policy. Wszelkie pytania dotyczące naszego Oświadczenia dotyczącego polityki równych szans zatrudnienia można kierować do osoby kontaktowej wskazanej w naszym Oświadczeniu dotyczącym polityki.

[Zależnie od przypadku] prosimy o podjęcie odpowiednich działań zgodnie z naszym Oświadczeniem dotyczącym polityki oraz naszymi regulacjami.

3 PRZECIWDZIAŁANIE ŁAPOWNICTWU I KORUPCJI (AB&C)

Firma Citi wdrożyła rozsądne zasady, procedury i kontrole wewnętrzne mające na celu zapewnienia zgodności z przepisami zwalczającymi łapownictwo i korupcję, dlatego surowo zabrania łapownictwa oraz ułatwiania przyjmowania korzyści materialnych w jakiegokolwiek formie. Dostawcy (w tym Pośrednicy biznesowi), ich Personel i wszystkie osoby działające w imieniu Citi, bezpośrednio lub pośrednio, będą prowadzić swoją działalność zgodnie z najwyższymi standardami etycznymi oraz zgodnie z amerykańską ustawą o zagranicznych praktykach korupcyjnych (FCPA), brytyjską ustawą antykorupcyjną (UKBA), włącznie z wszystkimi wprowadzanymi do nich zmianami, a także wszelkimi innymi obowiązującymi lokalnymi przepisami AB&C krajów, w których Citi prowadzi działalność.

Ani Dostawca, ani żaden z członków jego Personelu, działający w imieniu Citi lub w związku z jakąkolwiek umową Dostawcy lub relacjami z Citi, (i) nie dokona, nie przekaze, nie upoważni ani nie zaoferuje żadnych płatności, korzyści, przywilejów ani jakiegokolwiek innej wartościowej rzeczy jakiegokolwiek osobie; lub (ii) nie otrzyma ani nie przyjmie żadnej płatności, korzyści, przywileju ani jakiegokolwiek innej wartościowej rzeczy od jakiegokolwiek osoby, w każdym przypadku (i) (ii) z naruszeniem ustawy FCPA, ustawy UKBA lub innych przepisów AB&C. Dostawca i jego Personel muszą prowadzić działania własne i transakcje w imieniu Citi lub w związku z jakąkolwiek umową Dostawcy lub relacjami z Citi, zgodnie z Wymaganiami, w tym niniejszą Częścią. Dostawca i jego Personel muszą również utrzymywać program zgodności z przepisami AB&C oraz

polityki i procedury mające na celu zapewnienie zgodności z wszystkimi przepisami AB&C.

Omówienie programu przeciwdziałania łapownictwu i korupcji Citi opublikowano w witrynie [Citigroup's Investor Relations](#) (w sekcji Polityki Citi należy przejść do działu Program przeciwdziałania łapownictwu i korupcji).

4. PREZENTY I ROZRYWKA

Ani Dostawcy, ani ich Personel, nie mogą wręczać prezentów ani zapewniać żadnych korzyści osobistych lub majątkowych (w tym rozrywki) pracownikom Citi, jeżeli spowodowałyby to faktyczny lub pozorny konflikt interesów, sytuację „coś za coś”, zagroziłoby uczciwości lub osądowi pracownika lub w inny sposób niewłaściwie wpłynęłoby na proces decyzyjny pracownika, powodowałoby, że pracownik wykraczałby poza zakres swoich obowiązków, albo w inny sposób naruszyło obowiązujące przepisy. Nie ograniczając powyższych postanowień, pracownik musi przestrzegać Części dotyczącej zakazanych prezentów i rozrywki w ramach Standardu dotyczącego prezentów i rozrywki. Dostawcy i ich Personel nie mogą wręczać jakimkolwiek pracownikom Citi niepieniężnych prezentów o charakterze biznesowym o łącznej wartości przekraczającej 300 USD na osobę w roku kalendarzowym.

Gdy Dostawca sponsoruje pracownikowi Citi spotkanie służbowe (np. zaprasza na posiłek, wydarzenie sportowe, kulturalne lub inne podobne wydarzenie), Dostawca musi uczestniczyć w tym wydarzeniu, a impreza musi mieścić się w zwyczajowo przyjętych normach i nie przekraczać zwyczajowych granic, nie może być wystawna i nie może odbywać się nadmiernie często. Ponadto, jeśli Dostawca nie będzie obecny na wydarzeniu, rozrywka zostanie uznana za prezent biznesowy i będzie podlegać odpowiednim progom raportowania określonym w Standardzie Citi dotyczącym prezentów i rozrywki. Dostawca nie może przekazywać w imieniu Citi ani rzekomo w imieniu Citi żadnych korzyści majątkowych, w tym na własny koszt Dostawcy lub koszt pracownika Citi, jakiegokolwiek osobie, bezpośrednio ani pośrednio, ani nakłaniać innej osoby do takiego działania, jeśli takie działanie byłoby lub mogłoby być racjonalnie postrzegane jako korupcjogenne, niestosowne lub naruszające obowiązujące przepisy prawa.

5 ZAANGAŻOWANIE DOSTAWCÓW I ZASADY DLA DOSTAWCÓW

<https://www.citigroup.com/citi/suppliers/> Citi angażuje Dostawców w wiele inicjatyw i podnosi świadomość w zakresie programu zamówień Citi wśród potencjalnych Dostawców ze społeczności, którym służymy. Ponadto działania w zakresie zaangażowania mają na celu zidentyfikowanie obiecujących Dostawców, zwłaszcza tych, którzy tworzą innowacyjne rozwiązania w celu rozwiązania pojawiających się problemów biznesowych. Dodatkowe informacje na temat oczekiwań Citi wobec Dostawców można znaleźć w witrynie [Doing Business with Citi](#):

6 ZWALCZANIE WSPÓŁCZESNEGO NIEWOLNICTWA

Citi angażuje się w utrzymywanie praktyk, których celem ma być identyfikowanie ryzyka i zapobieganie przypadkom niewolnictwa lub handlu ludźmi w organizacji lub jakichkolwiek jej łańcuchach dostaw. Dostawcy Citi zobowiązani są do przestrzegania określonych poniżej Wymagań, a także do opracowania skutecznych polityk, procedur i/lub praktyk obejmujących całe przedsiębiorstwo, w celu identyfikacji ryzyka i zapobiegania przypadkom współczesnego niewolnictwa oraz handlu ludźmi w ramach swojej własnej działalności i łańcuchów dostaw. Dostawcy są zobowiązani do wypełnienia Kwestionariusza dotyczącego odpowiedzialności korporacyjnej Dostawcy (CRQ, Corporate Responsibility Questionnaire) Citi na żądanie Citi, oraz podania wszelkich niezbędnych informacji, aby umożliwić Citi ocenę narażenia na ryzyko i potencjalnych działań łagodzących, szczególnie w przypadku Dostawców z sektorów i obszarów geograficznych o podwyższonym ryzyku. Od Podwykonawców Dostawcy oczekuje się przestrzegania tego samego procesu.

6.1 Zakaz zatrudniania dzieci

Dostawcy nie mogą zatrudniać osób nieletnich. Termin „osoba nieletnia” odnosi się do osób poniżej minimalnego wieku zatrudnienia zgodnie z obowiązującymi przepisami prawa lub w przypadku braku takich przepisów, osób poniżej 15 roku życia lub poniżej wieku wymaganego do wywiązania się z obowiązku szkolnego, zależnie od tego, który wiek jest wyższy. Zgodnie z nadrzędnym zakazem zatrudniania osób nieletnich w przypadku zatrudniania pracowników poniżej 18 roku życia należy zwracać szczególną uwagę na wykonywane przez nich obowiązki oraz warunki, w których pracują, aby zapewnić, że takie osoby nie odnoszą żadnej krzywdy psychicznej, fizycznej ani żadnej innej wynikającej w sposób pośredni lub bezpośredni z ich pracy lub warunków pracy.

6.2 Swoboda wyboru zatrudnienia

Dostawca zapewni, że pracownicy nie będą zmuszani, fizycznie ani psychicznie przymuszani, zniewalani, objęci systemem pracy za długi ani poddawani niedobrowolnej pracy bądź niewolnictwu, nie będą przedmiotem handlu ludźmi ani nie będą poddawani przymusowej pracy w jakiejkolwiek formie, w tym w ramach obowiązkowych nadgodzin. Praca musi być wykonywana dobrowolnie. Zobowiązania Dostawcy wynikające z niniejszej Umowy obejmują między innymi:

1. **Umowy, wynagrodzenia i godziny pracy:** Pracownikom należy przedstawić warunki zatrudnienia lub współpracy w formie pisemnej, która jest dla nich zrozumiała i jasno opisuje ich prawa i obowiązki. Ten dokument pisemny będzie zawierać m.in. przejrzyste warunki dotyczące płacy, wynagrodzenia za nadgodziny, terminów płatności, godzin pracy oraz praw w odniesieniu do przerw na odpoczynek i urlopów. Takie warunki w formie pisemnej należy dostarczyć pracownikowi przed rozpoczęciem przez niego pracy. Muszą one być przestrzegane przez pracodawcę i spełniać standardy branżowe oraz

minimalne wymogi obowiązującego prawa oraz układów zbiorowych obowiązujące w miejscu wykonywania pracy.

2. **Prawo do swobodnego rozwiązania stosunku pracy:** Pracownicy muszą mieć prawo do swobodnego rozwiązania stosunku pracy z zachowaniem stosownego okresu wypowiedzenia zgodnego z obowiązującym prawem oraz układami pracy zbiorowej, bez nakładania na nich jakichkolwiek nieuzasadnionych kar.
3. **Nieludzkie traktowanie:** Pracownicy, ich rodziny i osoby blisko z nimi związane nie mogą być poddawani surowemu lub nieludzkemu traktowaniu, w tym między innymi karom cielesnym, przemocy fizycznej, psychicznej ani seksualnej, przymuszaniu, przemocy słownej, prześladowaniu ani zastraszaniu. Pracownicy migrujący, ich rodziny i osoby blisko z nimi związane nie mogą być przedmiotem dyskryminacji pod względem warunków zatrudnienia lub warunków pracy w związku z narodowością tych osób.
4. **Wynagrodzenia, świadczenia i godziny pracy:** Wynagrodzenie powinno być zgodne z wszystkimi obowiązującymi przepisami dotyczącymi płac, w tym regulującymi płacę minimalną, godziny nadliczbowe i prawnie przysługujące świadczenia. Pracownicy powinni otrzymywać wynagrodzenie w całości, terminowo i z przejrzystymi rozliczeniami wynagrodzeń. Nie dopuszcza się stosowania żadnych karnych potrąceń z wynagrodzenia lub świadczeń ani wstrzymywania ich jako środków dyscyplinarnych. Tydzień roboczy nie powinien przekraczać maksymalnego wymiaru godzin ustalonego przez prawo miejscowe, a praca w godzinach nadliczbowych musi być dobrowolna, w granicach prawa, a odmowa pracy w godzinach nadliczbowych nie może być karana.
5. **Zakaz konfiskowania dokumentów tożsamości:** Dokumenty tożsamości, zezwolenia na podróż, paszporty ani żadne inne dokumenty bądź rzeczy wartościowe należące do pracownika nie mogą być konfiskowane ani zatrzymywane jak warunek zatrudnienia, a zatrzymanie własności nie może być wykorzystywane, bezpośrednio ani pośrednio, do ograniczania wolności pracowników ani tworzenia warunków pracy o charakterze niewolnictwa.
6. **Brak opłat rekrutacyjnych i niewoli spowodowanej zadłużeniem:** Opłaty lub koszty związane z rekrutacją pracowników (w tym między innymi koszty wiz pracowniczych, koszty podróży oraz koszty przetwarzania dokumentów) nie będą bezpośrednio ani pośrednio przenoszone na pracowników. Nie wolno również wymagać od pracowników dokonywania opłat, w tym opłat zabezpieczających, których celem lub skutkiem będzie stworzenie warunków pracy o charakterze niewolnictwa, ani zmuszać ich do odpracowywania zadłużenia. W przypadku stwierdzenia, że w związku z procesem rekrutacji pracownicy zostali obciążeni kosztami lub opłatami albo w trakcie zatrudnienia zostały poniesione przez nich jakiegokolwiek koszty lub opłaty, Dostawca podejmie uzasadnione działania w celu bezzwłocznego zwrotu tych kosztów.

Jeśli zachodzi konieczność rekrutacji pracowników angażowanych za pośrednictwem strony trzeciej, takiej jak agencja pracy, należy współpracować wyłącznie z renomowanymi agencjami pośrednictwa pracy. W przypadku bezpośredniego zatrudniania pracowników należy współpracować wyłącznie z renomowanymi agencjami rekrutacyjnymi. Zakaz opłat rekrutacyjnych wnoszonych przez pracowników dotyczy wszystkich rekruterów, agentów i subagentów. Dostawcy muszą dysponować środkami kontroli zapewniającymi zgodność z wymaganiami. **Swoboda przemieszczania się:** Pracownicy powinni mieć swobodę przemieszczania się bez nieuzasadnionych ograniczeń i nie mogą być fizycznie przetrzymywani w miejscu pracy ani w żadnym innym miejscu kontrolowanym przez pracodawcę (np. w zakwaterowaniu pracowniczym). Na pracowników nie wolno nakładać obowiązku korzystania z zakwaterowania w obiektach kontrolowanych przez pracodawcę, chyba że jest to konieczne ze względu na miejsce lub charakter wykonywanej pracy.

7. **Skargi bez podejmowania działań odwetowych:** Pracownicy mają możliwość składania skarg do swojego pracodawcy w zakresie sposobu, w jaki są przez niego traktowani. Zgłoszenie skargi nie może wiązać się z poniesieniem przez pracownika negatywnych konsekwencji, doświadczeniem przez niego działań odwetowych ani represjonowania.

7 PERSONEL DOSTAWCY

7.1 Szkolenie, przydział, zmiana przydziału personelu i zarządzanie personelem Dostawcy

Dostawca zatrudni odpowiednią liczbę osób posiadających stosowne przeszkolenie, wykształcenie, doświadczenie i umiejętności w celu świadczenia Usług w najbardziej efektywny sposób zgodny z postanowieniami Umowy. Ponadto Dostawca uzasadni na żądanie kwalifikacje takich osób. Po przydzieleniu Personelu do Projektu Dostawca nie będzie przenosić ani wykorzystywać pracowników do innych zadań, które ograniczają ich dyspozycyjność do pracy nad Projektem bez uprzedniej pisemnej zgody Citi. Zasadniczo Dostawca będzie przydzielać Personel do Projektów w sposób minimalizujący zakłócenia spowodowane potrzebą reorientacji. Dostawca zapewni, że jego Personel nie będzie przedstawiać się jako pracownicy lub agenci Citi ani nie będzie starać się być traktowany jako pracownicy Citi w jakimkolwiek celu, włącznie z roszczeniami o prawo do świadczeń pracowniczych zapewnianych przez Citi, zasiłek z tytułu niezdolności do pracy, składki na ubezpieczenie zdrowotne lub świadczenia z tytułu zabezpieczenia społecznego, federalne podatki od bezrobocia (FUTA), stanowe podatki od bezrobocia (SUTA) lub federalne podatki potrącane u źródła. Dostawca ponosi wyłączną odpowiedzialność za wszystkie obowiązki pracodawcy związane z zatrudnieniem w odniesieniu do swojego Personelu, w tym m.in. za podtrzymywanie wszystkich wymaganych umów ubezpieczeniowych, składanie wszystkich stosownych deklaracji podatkowych oraz dokonywanie wszelkich wymaganych płatności i wpłat podatków w sposób zgodny ze statusem Dostawcy jako niezależnego wykonawcy.

7.2 Wymiana personelu Dostawcy

Dostawca usunie i zastąpi Personel przydzielony przez niego do Projektu, jeśli Citi powiadomi Dostawcę, że przyjęcie danego pracownika przez Citi jest niemożliwe z przyczyn o niedyskryminacyjnym charakterze. Dostawca zobowiązuje się ponadto do usunięcia i zastąpienia dowolnego Personelu przypisanego do Projektu oraz uniemożliwienia mu świadczenia Usług na rzecz Citi (lub pełnienia obowiązków w odniesieniu do świadczenia lub nadzoru Usług) niezwłocznie, gdy taka osoba nie jest w stanie lub nie chce świadczyć Usług terminowo i w sposób profesjonalny.

7.3 Polityka Dostawcy dotycząca personelu

Dostawca oświadcza, gwarantuje i potwierdza, że posiada oraz skutecznie wdraża kompleksowe polityki i procedury kwalifikowania swojego Personelu, który składa się z osób fizycznych i jest wyznaczony do świadczenia Usług na miejscu na rzecz Citi, oraz że te polityki i procedury obejmują weryfikację uprawnień do pracy, weryfikację historii zatrudnienia i wyroków skazujących, zgodnie z dalszymi postanowieniami niniejszego dokumentu, oraz badania na obecność narkotyków przed zatrudnieniem, w zakresie dozwolonym przez obowiązujące prawo i wszelkie obowiązujące układy zbiorowe. Nie ograniczając ogólnej wymowy powyższego, Dostawca oświadcza, gwarantuje i potwierdza również, że dysponuje środkami kontroli i procedurami zapewniającymi pełną zgodność Dostawcy z wszystkimi Obowiązującymi przepisami dotyczącymi imigracji, w tym potwierdza, że cały Personel Dostawcy przydzielony do Citi jest upoważniony do pracy w trakcie realizacji zadania, w pełnej zgodności ze wszystkimi Obowiązującymi przepisami dotyczącymi imigracji. Na żądanie Dostawca niezwłocznie dostarczy Citi pisemny dowód upoważnienia do pracy dla dowolnego pracownika lub całego Personelu Dostawcy przydzielonego do świadczenia usług na rzecz Citi oraz zgodność tego Personelu z Obowiązującymi przepisami dotyczącymi imigracji, a także zastąpi każdego pracownika bez zgodnego z Obowiązującym prawem upoważnienia do pracy odpowiednio wykwalifikowanymi pracownikami, w tym zapewni wszelkie niezbędne szkolenia w celu zapewnienia terminowego i skutecznego świadczenia Usług — w każdym przypadku bez dodatkowych kosztów dla Citi.

7.4 Odpowiedzialność Dostawcy

Aby zachować zgodność z obowiązującymi przepisami prawa i regulacjami w jurysdykcjach, w których Citi prowadzi działalność, na żądanie Citi Dostawcy są zobowiązani do przedstawienia szczegółów dotyczących właścicieli, którzy są osobami fizycznymi i/lub podmiotami prawnymi, w tym bezpośredniego właściciela (lub podmiotów) Dostawcy aż do poziomu obejmującego ostatecznego właściciela faktycznego, który sprawuje własność lub kontrolę, bezpośrednio lub pośrednio, poprzez wpływ lub inne środki, nad zaangażowaniem, produktem lub usługą.

8 PRZECIWDZIAŁANIE OSZUSTWOM

W związku z wysiłkami podejmowanymi przez Citi na rzecz identyfikacji i ograniczania ryzyka oszustw („Przeciwdziałanie oszustwom”)

8.1 Wszyscy Dostawcy będą:

1. Współpracować z Citi w każdym dochodzeniu dotyczącym podejrzenia lub zarzutu kradzieży, oszustwa lub innej potencjalnej działalności przestępczej lub wykroczenia, a także przy postępowaniach karnych dotyczących

oszustwa lub zachowania przestępczego w pełnym zakresie dozwolonym przez prawo.

2. Bezzwłocznie informować i zgłaszać do Citi potencjalne przypadki nadużyć za pomocą [Ethics Hotline](#). Obejmuje to między innymi próby, podejrzenia, domniemaną lub faktyczną kradzież, oszustwo (np. świadome podanie fałszywych, niedokładnych lub zmienionych danych dotyczących Dostawcy, schematów rozliczeniowych, ukrycia funduszy lub papierów wartościowych itp.), działalność przestępczą lub wykroczenia z udziałem Citi, pracownika Citi, Dostawcy lub przedstawiciela Citi albo osoby niebędącej pracownikiem Citi (np. pracownicy tymczasowi i kontrahenci).
3. Udzielać firmie Citi i jej przedstawicielom zgody na monitorowanie i nadzór oraz wspierać dochodzenia prowadzone przez Citi oraz organy ścigania w sprawie potencjalnych oszukańczych działań tego Dostawcy.
4. Terminowo zgłaszać wszelkie konflikty interesów (w tym konflikty interesów między Dostawcami / Pracownikami Dostawcy i/lub Pracownikami Citi), o których Dostawcy są informowani; oraz
5. Wspierać procesy Citi w zakresie zapobiegania oszustwom podczas zakładania lub aktualizowania konta bankowego Dostawcy w systemie płatności dla Dostawców Citi.

8.2 Ponadto Dostawcy świadczący usługi z natury bardziej narażone na ryzyko oszustwa zobowiązani są do:

1. Dokumentowania i przestrzegania Programu zarządzania ryzykiem oszustwa, który identyfikuje istotne ryzyko oszustw związane z usługami świadczonymi na rzecz Citi, a także mechanizmów kontroli i procedur wdrożonych w celu ograniczenia tego ryzyka.
2. Ukończenia szkolenia dotyczącego podnoszenia świadomości w zakresie oszustw (w ciągu 90 dni kalendarzowych od daty zatrudnienia, a następnie raz w roku) oraz przeszkolenia pracowników w zakresie konkretnych kwestii związanych z ryzykiem oszustwa dotyczących konkretnych usług świadczonych na rzecz Citi.
3. Monitorowania prób oszustwa i stosowania skutecznych mechanizmów kontroli w celu ograniczenia ryzyka oszustwa w usługach świadczonych na rzecz Citi, dokumentowanie procedur kontroli i bieżące testowanie skuteczności mechanizmów kontroli, zgłaszając wszelkie problemy Właścicielowi Działów Biznesowych (BAO).
4. Przekazywania wszelkich informacji wymaganych do analizy due diligence / stałego monitorowania / oceny narażenia Właściciela Działów Biznesowych (BAO) na ryzyko nadużyć.
5. Prowadzenia analizy due diligence obejmującej szablon oceny wpływu oszustw przez strony trzecie (Third-Party Fraud Impact Assessment Template, „TP-FIAT”), której celem jest przeprowadzanie ocen mechanizmów kontrolnych dotyczących możliwości Dostawców w zakresie ograniczania ryzyka oszustw. Ta procedura operacyjna opisuje zestaw kroków do podjęcia

przez Właściciela Działów Biznesowych (BAO) lub Specjalistę ds. podmiotów zewnętrznych (TPO) oraz Specjalistę ds. zarządzania ryzykiem oszustwa („FRMO”) w celu identyfikacji ryzyka oszustwa i zarządzanie nim.

8.3 Dostawcy o wyższym ryzyku inherentnym oszustwa to między innymi Dostawcy, którzy:

1. mają dostęp do danych sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności (jeżeli nie są one pod bezpośrednią kontrolą lub nadzorem Citi), które mogą być wykorzystane do popełnienia oszustwa, jak dostęp do kont wewnętrznych, transakcji finansowych, transakcji gotówkowych;
2. mają łączność z sieciami/systemami Citi; oraz
3. zapewniają, wspierają lub mają dostęp do usług i funkcji, które mogłyby być wykorzystane do popełnienia oszustwa lub umożliwienia popełnienia oszustwa, w tym:
 - a) Identyfikacja, nawiązywanie współpracy lub przetwarzanie wniosków od nowych klientów.
 - b) Działania związane z płatnościami / transferem funduszy Citi lub Klientów i/lub uwierzytelnianie Klientów Citi, którzy mają dostęp do tych usług;
 - c) Wprowadzanie, sprawdzanie lub realizacja zmian w danych należących do Citi lub Klientów Citi (np. danych demograficznych);
 - d) Zapewnianie, obsługi lub autoryzacji instrumentów transakcyjnych (np. kart debetowych/kredytowych, portfeli elektronicznych, książeczek czekowych itp.);
 - e) Oferowanie lub wspieranie działań operacyjnych w zakresie zarządzania ryzykiem oszustw na rzecz Citi, związanych z zapobieganiem, wykrywaniem lub reagowaniem na oszustwa;
 - f) Zapewnianie fizycznego dostępu do gotówki, instrumentów finansowych i aktywów / dóbr materialnych;
 - g) Dostęp bez eskorty lub poza godzinami pracy w obiektach Citi;
 - h) Sprawozdania finansowe: działalność rachunkowo-księgowa, na przykład księgowanie wpisów w księdze głównej / księdze pomocniczej;
 - i) Zdobywanie i wydawanie nagród za działania motywacyjne.

9 KONTAKTY Z MEDIAMI I WYSTĄPIENIA PUBLICZNE

Citi Enterprise Services and Public Affairs to jedyny oddział Citi uprawniony do wydawania komunikatów prasowych lub publicznych oświadczeń w imieniu Citi. Dostawcy nie mogą wydawać żadnych komunikatów prasowych, które bezpośrednio lub pośrednio potwierdzają powiązanie z Citi, zawarcie jakichkolwiek umów lub porozumień pomiędzy Dostawcą a Citi lub zamówienie produktów lub usług u Dostawcy przez Citi. Dostawcy nie mogą wyrażać zgody na ani angażować się w jakiegokolwiek działania w zakresie PR (ang. public relations) dotyczących Citi z klientami, pracownikami Citi, innymi Dostawcami Citi, innymi klientami Dostawców lub innymi osobami trzecimi bez uprzedniej pisemnej zgody głównej osoby ds. kontaktów biznesowych Citi.

Dostawcy nie mogą publikować ani zamieszczać żadnych materiałów w formie pisemnej ani elektronicznej (dotyczy to książek, artykułów, podcastów, webcastów, blogów, informacji w witrynach internetowych, fotografii, materiałów wideo, mediów społecznościowych oraz innych mediów), wygłaszać przemówień, udzielać wywiadów ani brać udziału w wystąpieniach publicznych, w których mowa o Citi, działaniach Citi, jej Klientach, produktach lub usługach, bez uzyskania uprzedniej pisemnej zgody głównej osoby do kontaktu w jednostce biznesowej Citi oraz starszego pracownika krajowego biura spraw publicznych.

Niezależnie od tego, czy jest to związane ze świadczeniem usług lub dostarczaniem produktów na rzecz Citi, Dostawcy nie mogą korzystać z zastrzeżonych oznaczeń Citi, znaków towarowych, znaków usługowych, nazw handlowych, logo, symboli ani nazw marek, bez każdorazowego uzyskania uprzedniej pisemnej zgody Citi. Dostawcy nie mogą wykorzystywać nazwy Citi, jej logo, znaków towarowych, placówek ani kontaktów dla własnych korzyści ani na potrzeby pracy niezwiązanej z Citi (dotyczy to informacji przekazywanych na papierze firmowym lub w osobistych witrynach internetowych, na blogach lub w innych serwisach społecznościowych). Ponadto Dostawcy nie mogą w żaden sposób wykorzystywać nazwy, placówek ani kontaktów Citi w celach charytatywnych ani w działalności pro bono.

10 PISEMNA KOMUNIKACJA ELEKTRONICZNA

W kontaktach z pracownikami Citi lub w trakcie wykonywania obowiązków na rzecz lub w imieniu Citi Dostawcy mogą korzystać wyłącznie z tych Urządzeń, Systemów i Usług Komunikacji elektronicznej zapisywanych w formie tekstowej, które zostały zatwierdzone przez Citi. Korzystanie z nowych, rozszerzonych lub zmienionych kanałów korespondencji elektronicznej Citi, jako narzędzi samodzielnych lub zintegrowanych z szerszą platformą, dostarczonych przez Citi lub stronę trzecią, musi zostać zatwierdzone zgodnie ze stosownymi Wymaganiami Citi, o których Dostawca został powiadomiony w pisemnym powiadomieniu BAO. Omawianie kwestii dotyczących działalności Citi między pracownikami za pośrednictwem niezatwierdzonych przez Citi platform komunikacyjnych, takich jak WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber i inne interaktywne platformy elektroniczne, jest zabronione.

Ponadto Dostawcy nie powinni oczekiwać prywatności w odniesieniu do pisemnej Komunikacji elektronicznej tworzonej, ujawnianej, używanej, uzyskiwanej, pobieranej, przechowywanej, przesyłanej, otrzymywanej lub usuwanej za pośrednictwem Urządzeń, Systemów i Usług komunikacyjnych dostarczanych przez Citi. Citi może monitorować Urządzenia, Systemy i Usługi Komunikacji elektronicznej oraz Komunikację elektroniczną. Taka Komunikacja elektroniczna stanowi własność Citi i może być przechowywana zgodnie z obowiązującymi procedurami przechowywania danych rejestrowych (zgodnie z lokalnymi przepisami prawa).

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

11 DZIAŁALNOŚĆ POLITYCZNA I FINANSOWANIE KAMPANII

Różne przepisy prawne, takie jak zasady dotyczące: wpływów zagranicznych; finansowania kampanii; prezentów i rozrywki; lobbingu legislacyjnego, oddolnego, wizerunkowego i regulacyjnego; zamówień publicznych; oferowania usług za opłatą (pay-to-play); oraz obrotu papierami wartościowymi, regulują działalność polityczną firmy Citi i jej Dostawców. Wszelka działalność polityczna Dostawców, która nie jest zgodna z polityką lub standardami Citi, obowiązującym prawem lub regulacjami, jest zabroniona.

Działalność polityczna obejmuje m.in.:

1. Przekazywanie firmowych lub osobistych datków na cele polityczne, zabieganie o datki na cele polityczne, wykorzystywanie funduszy lub zasobów Citi (takich jak placówki, wyposażenie, oprogramowanie lub personel) lub też dobrowolne oferowanie swych usług w czasie pracy osobie ubiegającej się o urząd publiczny, komitetowi partii politycznej lub komitetowi politycznemu
2. Działania lobbingowe lub angażowanie się w działania na rzecz urzędników państwowych, bezpośrednio lub za pośrednictwem osób trzecich, w tym próby wpływania na urzędników, ustawodawców; w zależności od jurysdykcji działalność polityczna może również obejmować próby wywierania wpływu na organy ustawodawcze lub zarządzające przetargami na zlecenia rządowe
3. Ubieganie się o stanowisko polityczne, przyjmowanie nominacji na stanowisko polityczne lub piastowanie stanowiska politycznego w rządzie, w tym we wszelkich radach rządowych, komisjach lub innych podobnych organach

Ponadto żaden Dostawca nie może podejmować ani prowadzić żadnej działalności politycznej w imieniu (lub rzekomo w imieniu) Citi lub jej klientów bez uzyskania uprzedniego pisemnego upoważnienia od Globalnego działu Citi ds. kontaktów z podmiotami rządowymi (Government Affairs Global Operations Control) (ggacontrol@citi.com). Citi ma prawo dokonywać opłat i/lub zwracać koszty własne za usługi w zakresie działalności politycznej świadczone przez Dostawcę na podstawie umowy i zgodne z przepisami, takie jak lobbing, jednak Citi nigdy nie zwraca Dostawcy ani jego pracownikom żadnych wydatków poniesionych z tytułu osobistych lub firmowych datków na cele polityczne.

12 PRZECIWDZIAŁANIE PRANIU PIENIĘDZY („AML”)

Dotyczy Dostawców świadczących konkretne usługi związane z obsługą klientów (na przykład proces wdrażania nowych pracowników, monitorowanie kont klientów i transakcji finansowych) lub dostarczających dane/wskaźniki związane z powyższymi czynnościami; I/LUB pełniących funkcję pośrednika w odniesieniu do transakcji lub instrumentów finansowych (np. zdalne przyjmowanie depozytów, usługi kurierskie, obsługa samochodów opancerzonych lub skrytek, transfery elektroniczne, zasoby cyfrowe).

12.1 Obowiązki związane z AML:

1. Zgodność z Procesami Citi oraz obowiązującymi przepisami prawa:

- Przestrzeganie procesów i procedur Citi mających na celu spełnienie wymagań wynikających z obowiązujących przepisów, w tym (i) amerykańskiej ustawy Gramm-Leach-Bliley Act oraz przepisów wydanych na jej podstawie; (ii) amerykańskiej ustawy PATRIOT Act oraz przepisów wydanych na jej podstawie; (iii) wszelkich przepisów prawnych i regulacji dotyczących prania pieniędzy oraz (iv) wszelkich przepisów prawnych i regulacji dotyczących sankcji gospodarczych. Takie polityki i procedury będą regulować role i obowiązki związane z przeciwdziałaniem praniu pieniędzy, w tym wymagania dotyczące niezwłocznego zgłaszania wszelkich zaobserwowanych działań, które wydają się nietypowe lub potencjalnie nietypowe w związku z działalnością finansową, transakcjami oraz przyjmowaniem gotówki.

2. Coroczne szkolenia i elementy programu dla personelu:

- Zapewnienie Personelowi świadczącemu usługi na rzecz Citi corocznych szkoleń dotyczących ról i obowiązków związanych z przeciwdziałaniem praniu pieniędzy, w tym wymagań dotyczących niezwłocznego zgłaszania wszelkich zaobserwowanych działań, które wydają się nietypowe lub potencjalnie nietypowe w związku z działalnością finansową, transakcjami oraz przyjmowaniem gotówki. Szkolenia będą obejmować między innymi następujące komponenty:
 - a. Zgłaszanie i eskalacja podejrzanych działań.
 - b. Program „Poznaj swojego klienta” (KYC, Know Your Customer), w tym Program Identyfikacji Klienta (CIP, Customer Identification Program), sankcje i weryfikacja tożsamości oraz procedury zachowania wobec klienta należytej staranności (CDD, Customer Due Diligence), zwiększonej należytej staranności (EDD, Enhanced Due Diligence) oraz identyfikacja i weryfikacja **Ostatecznych Właścicieli Faktycznych (UBO, Ultimate Beneficial Owner)**.
 - c. Monitorowanie transakcji we wszystkich istotnych instrumentach i działaniach finansowych.
 - d. Okresowe raportowanie/wskaźniki, w tym raportowanie dotyczące zmian prawnych i regulacyjnych oraz istotnych zmian programu AML.
 - e. Testowanie i kontrola skuteczności programu przeciwdziałania praniu pieniędzy, w tym wizyty na miejscu.

3. Zgodność z postanowieniami Umowy:

- Przestrzeganie wszelkich postanowień Umowy definiujących dowolny program, który musi zostać wprowadzony przez Dostawcę.

4. Niezwłoczne zgłaszanie domniemanych przypadków naruszeń:

- Niezwłoczne powiadamianie Citi na piśmie o wszelkich domniemanych przypadkach naruszenia prawa, w tym o wszelkich zaobserwowanych działaniach, które wydają się nietypowe lub potencjalnie nietypowe w związku z przyjmowaniem gotówki, działalnością finansową lub transakcjami z udziałem firmy Citi lub jej klientów.

5. Zapobieganie uchylaniu się od opodatkowania i raportowanie:

- Przestrzeganie wszystkich obowiązujących przepisów i regulacji podatkowych w krajach, w których prowadzą działalność.
- W żadnym przypadku Dostawcy nie powinni angażować się w umyślne niezgodne z prawem uchylanie się od opodatkowania ani ułatwiać takiego uchylania się innym osobom, na przykład przez angażowanie się w działania, które pomogłyby w uchylaniu się od płacenia należnych podatków lub ukrywaniu informacji przed organami podatkowymi.
- W związku z powyższym Dostawcy wdrożą właściwe procedury prewencyjne uniemożliwiające uchylanie się od płacenia podatków i będą niezwłocznie pisemnie zgłaszać do Citi wszelkie naruszenia lub podejrzenia naruszeń procedur dotyczących Citi.

12.2 Polityki i procedury wewnętrzne Dostawcy:

Dostawcy muszą przestrzegać wszelkich stosownych polityk i procedur wewnętrznych w celu zapewnienia zgodności z wszystkimi obowiązującymi obecnie lub wprowadzonymi w przyszłości przepisami i regulacjami dotyczącymi przeciwdziałania praniu pieniędzy.

13 ZARZĄDZANIE DOKUMENTACJĄ

Dotyczy Dostawców, którzy uzyskują dostęp do Informacji Citi, przetwarzają je lub je przechowują.

Citi wymaga, aby wszyscy Dostawcy sprawujący pieczę nad Informacjami Citi współpracowali ze stosownym Właścicielem Działów Biznesowych („BAO”) lub z główną osobą kontaktową w Citi w celu (i) identyfikowania i klasyfikowania Informacji jako Dokumentacji lub Informacji przejściowych na potrzeby zarządzania dokumentacją Citi, (ii) klasyfikowania Dokumentacji zgodnie z Głównym Katalogiem Dokumentacji Citi („MRC”), (iii) przechowywania Informacji zgodnie z wymaganiami Citi dotyczącymi

przechowywania oraz (iv) należytego usunięcia Informacji po zakończeniu Cyklu życia informacji w przypadku braku Nakazu zachowania informacji.

BAO lub główna osoba kontaktowa w Citi musi współpracować z Dostawcą w celu zapewnienia, że Dostawca zidentyfikował i sklasyfikował dokumentację zgodnie z kodami dokumentacji Citi znajdującymi się w Głównym Katalogu Dokumentacji oraz że Rejestr jest aktualizowany co najmniej raz w roku. Dostawca jest zobowiązany do przestrzegania wymogów z zakresu Zarządzania dokumentacją, przedstawionych mu przez BAO. Dokumenty spełniające kryteria kwalifikowalności do usunięcia muszą być odpowiednio i możliwie najszybciej usunięte, ale nie później niż sześć miesięcy po spełnieniu wymogów dotyczących przechowywania, o ile nie ma zastosowania Nakaz zachowania informacji. Informacje przejściowe muszą zostać zniszczone nie później niż dwa lata po ich ostatnim użyciu, chyba że podlegają Nakazowi zachowania informacji. Informacje przejściowe zawierające dane osobowe należy usunąć po osiągnięciu celu, do którego zostały zebrane, chyba że podlegają Nakazowi zachowania informacji. Dostawca musi zawiesić niszczenie Informacji Citi lub wprowadzanie do nich zmian, gdy zostanie powiadomiony o Nakazie zachowania informacji. W przypadku wątpliwości Dostawca powinien skontaktować się ze stosowną główną osobą kontaktową w Citi lub z BAO.

Co kwartał zasady przechowywania wymienione w Krajowych harmonogramach przechowywania dokumentacji są weryfikowane i w razie potrzeby aktualizowane w celu zachowania zgodności ze zmianami regulacyjnymi i wewnętrznymi DRIM. W przypadku zmiany, która ma wpływ na Dostawcę, BAO będzie służyć Dostawcy doradztwem. Dostawca oceni wpływ i wdroży zmiany w odpowiednich systemach, procesach, zasobach i Rodzajach dokumentacji, które posiada i którymi zarządza, w ciągu 90 dni od powiadomienia otrzymanego od BAO.

Dostawcy przechowujący dokumentację w imieniu Citi są odpowiedzialni za przechowywanie, gromadzenie i przedstawianie wszelkich Informacji uznanych za istotne dla postępowania prawnego/sądowego lub innego w wymaganym czasie zgodnie z żądaniem BAO. Dostawca musi, na żądanie, zwrócić informacje Citi wymagane zgodnie z obowiązującymi warunkami umownymi. Dostawcom nie wolno usuwać żadnych Informacji Citi, niezależnie od klasyfikacji tych informacji (np. Poufne, Niepoufne) bez uzyskania zgody głównej osoby kontaktowej w Citi lub BAO. Zgoda ta musi uwzględniać potwierdzenie, że Informacje przeznaczone do usunięcia nie podlegają istniejącemu Nakazowi zachowania informacji. Wymagania w zakresie Zarządzania dokumentacją i przechowywania dokumentacji oraz wszelkie inne wymogi dotyczące postępowania z informacjami będą obowiązywać także po rozwiązaniu lub wygaśnięciu Umowy, chyba że wyraźnie uzgodniono inaczej.

Dostawcy mają obowiązek prowadzenia dokumentacji zawierającej wykaz całego Personelu Dostawcy odpowiedzialnego za nadzorowanie zarządzania Informacjami Citi będącymi w posiadaniu Dostawcy oraz organizowania okresowych spotkań z główną

osobą kontaktową w Citi lub Specjalistą ds. zarządzania dokumentacją w celu przeglądania i aktualizowania nazwisk osób kontaktowych, szczegółów procedur, ról i obowiązków oraz Rejestru dokumentów Dostawcy Citi.

14 ODPORNOŚĆ PRZEDSIĘBIORSTWA / CIĄGŁOŚĆ DZIAŁALNOŚCI BIZNESOWEJ

Dotyczy Dostawców, którzy świadczą usługi lub hostują infrastrukturę technologiczną / aplikacje wykorzystywane przez Citi. Właściciel Działów Biznesowych Citi (BAO) jest odpowiedzialny za przekazanie Dostawcy informacji o możliwości zastosowania i wymaganiach COB.

14.1 Zasoby służące przywróceniu działania

Plan przywrócenia ciągłości operacyjnej Dostawcy musi uwzględniać alternatywne zasoby pozwalające na dostarczanie Citi wszystkich produktów i usług w przypadku, gdy pierwotne miejsca działalności Dostawcy zostaną pozbawione możliwości działania. Zasoby służące przywróceniu działania muszą być położone w miejscach geograficznie oddalonych od pierwotnych miejsc działalności, na tyle, by zminimalizować lub wyeliminować groźbę ponownego zaburzenia pierwotnego i awaryjnego miejsca działalności przez to samo zdarzenie.

1. Zasoby służące przywróceniu działania to nie tylko Systemy Informatyczne, lecz także wszelkie zasoby potrzebne do dalszego dostarczania Citi produktów i usług, w tym pracownicy, budynki, sprzęt biznesowy, centra obsługi danych, sieci danych i głosowe oraz usługi transportowe.
2. Dostawcy aplikacji mogą wdrożyć architekturę typu Hot/Hot (aktywny-aktywny) w celu zapewnienia konfiguracji wysokiej dostępności (HA). Architektura ta wymaga co najmniej dwóch identycznie skonfigurowanych systemów, które są uruchomione i dostępne dla klientów/użytkowników. Najważniejszą cechą oferowaną przez ten model jest to, że alternatywne środowiska działają równolegle z głównym (produkcyjnym) centrum danych.

14.2 Poziomy usług przywracania działania

Ciągłość działalności Dostawcy musi odpowiadać wymaganemu poziomowi usług, jeśli Citi ma uznać ją za skuteczną. Plan przywrócenia ciągłości operacyjnej Dostawcy powinien co najmniej określać konkretne wartości dla poniższych pozycji:

1. Docelowy czas przywrócenia działania
2. Docelowy punkt przywrócenia działania
3. Zasoby służące przywróceniu działania / wydajność technologiczna
4. Czas trwania przywracania

14.3 Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej

Dostawca będzie utrzymywać Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej w celu kontynuacji działalności (oraz dostarczy dowody przeprowadzania przez siebie bieżących i okresowych testów na żądanie Citi), tak aby

mimo jakichkolwiek zakłóceń w zdolności Dostawcy do dostarczania Produktów / świadczenia Usług lub wykonywania swoich innych zobowiązań wynikających z niniejszej Umowy w dowolnej lokalizacji lub dzięki wysiłkom określonych osób, Dostawca mógł niezwłocznie dostarczać Produkty / świadczyć Usługi i wykonywać swoje zobowiązania z innej lokalizacji lub z zastępczym Personalem. Kopię Planu przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej należy dostarczyć Citi w ciągu dziesięciu (10) dni kalendarzowych od Daty wejścia w życie każdego Zlecenia pracy zawartego między Citi a Dostawcą, a następnie corocznie przez okres, w którym obowiązuje każde Zlecenie pracy. Dostawca przekaze Citi wszelkie instrukcje lub inne informacje niezbędne Citi do dalszego korzystania z Produktów/Usług ze strony Dostawcy w okolicznościach, w których Dostawca powołuje się na swój Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej. Dostawca oświadcza, gwarantuje i potwierdza, że jego Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej będzie zawierać co najmniej:

1. Procedury i strategie przywracania działania, w tym zmianę lokalizacji, przekazywanie pracy i/lub zdalny dostęp w celu złagodzenia skutków zakłóceń, w tym niedostępności technologii (ataki typu odmowa usługi / DoS), niedostępności pierwotnego miejsca pracy (ataki typu odmowa dostępu / DoA), niedostępności pracowników (w tym podwykonawców);
2. Utrzymywanie przez Dostawcę (między innymi) ośrodka do odtwarzania awaryjnego innego niż lokalizacje Produktu/Usługi, przechowywanie nośników kopii zapasowych w lokalizacji innej niż lokalizacje Produktu/Usługi, korzystanie z zapasowych linii komunikacyjnych i serwerów;
3. Procedury tworzenia kopii zapasowych / przywracania działania i stosowania Produktów / Usług, w tym szczegółowy, udokumentowany plan reagowania na przedłużające się zakłócenia w Produktach / Usługach spowodowane awarią zasilania, awarią systemu, klęską żywiołową lub innymi nieprzewidzianymi okolicznościami, który obejmuje procesy i procedury wznowienia działalności we wspólnie uzgodnionym terminie;
4. Procedury ochrony całej treści;
5. Procedury i wszelkie umowy ze stronami trzecimi na sprzęt zastępczy (np. sprzęt komputerowy);
6. Procedury dla zewnętrznych zakładów produkcyjnych; oraz
7. Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej Dostawcy obejmie następujące zobowiązania:
 - a. Dostawca niezwłocznie powiadomi Citi o każdej sytuacji kryzysowej, która może mieć negatywny wpływ na Produkty/Usługi;
 - b. Dostawca przedstawi Citi w ciągu 24 godzin od wspomnianego powiadomienia plan dalszego dostarczania Produktów / świadczenia Usług w alternatywnym zakładzie przetwarzania;
 - c. Produkty/Usługi muszą być w pełni użyteczne w ciągu wymaganego Docelowego czasu przywrócenia działania (RTO,

Recovery Time Objective), który, o ile nie zdefiniowano inaczej w odpowiedniej Umowie, wynosi maksymalnie 4 godziny w przypadku procesów, które Citi ocenia na poziomie krytyczności „Krytyczny dla przedsiębiorstwa” lub „WYSOKI”; wynosi maksymalnie 24 godziny w przypadku procesów, które Citi ocenia na poziomie krytyczności „ŚREDNI”; oraz maksymalnie 72 godziny w przypadku procesów, które Citi ocenia na poziomie krytyczności „NISKI”; oraz

- d. Jeśli część obiektów Dostawcy stanie się niedostępna, Dostawca zobowiązuje się traktować Citi nie mniej korzystnie niż swoich innych klientów komercyjnych.

14.4 Wymagania Planu przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej mające zastosowanie do Usług hostowanych

W zakresie, w jakim Dostawca zarządza Usługą hostowaną i świadczy ją na rzecz Citi, obowiązują również poniższe postanowienia. Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej będzie zawierać co najmniej:

1. Procedury tworzenia kopii zapasowych / przywracania działania i stosowania Usług hostowanych, w tym szczegółowy, udokumentowany plan reagowania na przedłużające się zakłócenia w usługach spowodowane awarią zasilania, awarią systemu, klęską żywiołową lub innymi nieprzewidzianymi okolicznościami, który obejmuje procesy i procedury wznowienia działalności we wspólnie uzgodnionym terminie;
2. Co więcej, Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej Dostawcy obejmie następujące zobowiązania: (a) Dostawca powiadomi Citi na piśmie w ciągu dwóch (2) godzin o każdej sytuacji kryzysowej, która może mieć negatywny wpływ na Usługi hostowane; (b) przedstawi Citi w ciągu 24 godzin od wspomnianego powiadomienia plan dalszego świadczenia Usług w alternatywnym zakładzie przetwarzania, oraz (c) Usługi hostowane są w pełni operacyjne w ciągu 48 godzin od pierwszego powiadomienia.
3. Dostawca zgadza się udostępnić, na żądanie, informacje niezbędne do umożliwienia Citi opracowania planu przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej oraz planu ciągłości działalności biznesowej, który będzie funkcjonować wraz z Planem przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej Dostawcy oraz planem zachowania ciągłości działalności biznesowej; oraz
4. Jeśli część obiektów Dostawcy stanie się niedostępna, Dostawca zobowiązuje się traktować Citi nie mniej korzystnie niż swoich innych klientów komercyjnych.

14.5 Zmiany w Planie przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej

Dostawca może wprowadzać zmiany do swojego Planu przywrócenia ciągłości operacyjnej, o ile takie zmiany nie pogorszą skuteczności Planu przywrócenia ciągłości

operacyjnej w sposób, który mógłby negatywnie wpłynąć na usługi (np. wydłużenie RTO). Dostawca niezwłocznie poinformuje Citi o wszelkich zmianach w swoim Planie przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej i, na żądanie Citi, wyjaśni zmiany, tak aby firma Citi w pełni je zrozumiała i była w stanie na nie zareagować.

14.6 Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej **Podwykonawcy**

Dostawca zapewni, że każdy Podwykonawca Dostawcy będzie utrzymywać Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej i powiązane środki kontroli ciągłości działalności biznesowej zgodnie z Wymaganiami Citi dla Dostawców. Dostawca musi zapewnić odpowiedni nadzór nad Podwykonawcami, w tym okresowy przegląd takich środków kontroli i wyników testów, oraz zapewnić terminowe usuwanie wszelkich zidentyfikowanych luk.

14.7 Uruchomienie Planu przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej i powiadomienie o sytuacji kryzysowej

Dostawca niezwłocznie powiadomi główną osobę kontaktową w Citi:

1. Gdy Dostawca uruchomi Plan przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej; oraz
2. O wszelkich sytuacjach kryzysowych, zagrożeniach, ostrzeżeniach lub incydentach cybernetycznych wobec Dostawcy lub jego Podwykonawców, które mogą mieć niekorzystny wpływ na usługi lub produkty świadczone na rzecz Citi.

14.8 Testowanie

Wszystkie zasoby służące przywróceniu działania oraz plany Dostawcy muszą być testowane w ciągu 120 dni od wdrożenia produkcji (90 dni w przypadku aplikacji sklasyfikowanych przez Citi jako te o znaczeniu krytycznym dla przedsiębiorstwa) i być testowane co najmniej raz w roku (co 12 miesięcy). Testy muszą wykazać, że Dostawca jest w stanie przywrócić działanie na wymaganym poziomie w przypadku wszystkich produktów i usług świadczonych Citi. Testy te muszą być kompleksowe i obejmować pełen zakres Usług świadczonych na rzecz Citi. Dostawcy muszą powiadomić Citi o przeprowadzaniu testu przywrócenia produktów / usług dostarczanych lub świadczonych Citi z wyprzedzeniem co najmniej 30 dni kalendarzowych. Citi może brać udział w przeprowadzanych przez Dostawcę testach przywrócenia działania aplikacji wykorzystywanych przez Citi do sprawdzania funkcjonalności biznesowych aplikacji w środowisku przywracania działania, lub też obserwować takie testy. Jeśli Citi wyrazi chęć uczestnictwa w teście, przed przeprowadzeniem testu Dostawca dostarczy Citi cele testu, plan testu i procedury połączenia się ze stroną testową. W ciągu dziesięciu (10) roboczych dni po zakończeniu każdego testu Dostawca dostarczy Citi podsumowanie celów testów, plan testów oraz wyniki testów, w tym ramy czasowe wymagane do przywrócenia funkcji biznesowych oraz dowody wyników testów (np. zrzuty ekranu).

14.9 Weryfikacja wolumenu

Dostawca, który zajmuje się hostingiem aplikacji sklasyfikowanych przez Citi jako te o znaczeniu krytycznym dla przedsiębiorstwa, musi wykazać, że wolumeny produkcyjne

mogą być przetwarzane w jego środowisku COB / przywrócenia ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej. Citi i Dostawca muszą uzgodnić metodologię, która będzie stosowana do walidacji.

14.10 Wykorzystywanie systemów Citi do świadczenia Usług

Na żądanie Citi lub Podmiotów stowarzyszonych Citi Dostawcy korzystający z Systemów Citi będą uczestniczyć, bez ponoszenia przez Citi kosztów czy opłat, w wykonywanych przez Citi ćwiczeniach przywracania ciągłości operacyjnej po wystąpieniu sytuacji kryzysowej.

14.11 Podjęcie działań na podstawie wyników testów

Jeżeli wyniki testów przeprowadzonych przez Dostawcę wykażą niespełnienie któregoś z celów testów lub obowiązującego RTO, Dostawca przeprowadzi analizę przyczyn źródłowych i niezwłocznie usunie wszelkie zidentyfikowane problemy. Po wdrożeniu tych środków zaradczych Dostawca ponownie przeprowadzi test nie później niż sto dwadzieścia (120) dni kalendarzowych (90 dni kalendarzowych w przypadku aplikacji sklasyfikowanych przez Citi jako te o znaczeniu krytycznym dla przedsiębiorstwa) po pierwszym teście zakończonym niepowodzeniem (lub w terminie określonym w odpowiednim Zleceniu pracy).

14.12 Zarządzanie kryzysowe

Oprócz planu ciągłości działania Dostawca powinien posiadać plan zarządzania kryzysowego opisujący kierowanie operacjami przywrócenia działania i nadzorowanie ich. Plan taki powinien co najmniej wskazywać osoby o pozycji wystarczającej do rozpoczęcia operacji przywrócenia działania, określać protokoły komunikacyjne i eskalowania służące zbieraniu i rozpowszechnianiu informacji o kryzysie oraz zawierać protokoły powiadamiania i eskalowania służące komunikacji z Citi na wypadek kryzysu.

14.13 Oceny ciągłości działania

Dostawcy podlegają opracowanemu przez Citi Procesowi oceny ciągłości działalności biznesowej, który ma na celu ocenę polityk, procedur i środków kontroli wdrażanych przez Dostawców i dotyczących przestrzegania wymogów Citi oraz wszelkich wymogów prawnych i/lub regulacyjnych (obowiązujących Citi lub Dostawców), które odnoszą się do utrzymania ciągłości działalności biznesowej. Ocena składa się z kwestionariuszy wymagających od Dostawcy udzielenia odpowiedzi oraz dostarczenia dowodów pomocniczych i może obejmować wizyty w miejscach Dostawcy. Jeśli wyniki oceny ujawnią lub wykażą problemy lub kwestie związane z ciągłością działania, Citi udokumentuje takie wyniki i będzie współpracować z Dostawcą nad ustaleniem rozwiązań takich problemów. Dostawcy muszą szybko wprowadzić konieczne rozwiązania i/lub dodać lub skompensować środki kontroli w celu zajęcia się obawami Citi w zakresie satysfakcjonującym dla Citi.

14.14 Odporność operacyjna

Krytyczne usługi biznesowe to usługi, które w przypadku zakłócenia dostawy mogą mieć istotny negatywny wpływ na firmę Citi, jej klientów lub system finansowy. Dostawca dopilnuje, aby wszelkie zakłócenia w dostarczaniu elementów usług, które stanowią krytyczne usługi biznesowe lub wspierają świadczenie krytycznych usług biznesowych przez Citi, zgodnie z okresowymi wytycznymi Citi („Krytyczne usługi biznesowe”), nie

przekraczały czasu trwania określonego przez Citi ani nie naruszały w inny sposób stosownych wskaźników określonych przez Citi („Tolerancja wpływu”), o których Dostawca jest okresowo powiadamiany. Tolerancja wpływu będzie wyrażona jako precyzyjny wskaźnik oznaczający ilość czasu, w przypadku którego świadczenie usługi może zostać zakłócone. Citi i Dostawca będą dokonywać corocznego przeglądu Tolerancji wpływu w ramach bieżącego procesu zarządzania umowami. Jeśli firma Citi jest zobowiązana do ustalenia co najmniej jednej Tolerancji wpływu dla pojedynczej Krytycznej usługi biznesowej ze względu na wymagania więcej niż jednego Organu regulacyjnego, Citi może określić oddzielne Tolerancje wpływu dla takiej Krytycznej usługi biznesowej. Dostawca powinien:

1. Powiadomić Citi, gdy tylko dowie się, że nie udało się (lub prawdopodobnie nie uda się) dostarczyć jakiegokolwiek usługi w ramach odpowiedniej Tolerancji wpływu określonej przez Citi. Dostawca poda również wyjaśnienie przyczyn wszelkich potencjalnych lub rzeczywistych niepowodzeń i przedstawi kroki podjęte w celu złagodzenia skutków takiego niepowodzenia;
2. Na żądanie zapewnić firmie Citi uzasadnioną pomoc, aby umożliwić jej zidentyfikowanie osób, procesów, technologii, obiektów i informacji niezbędnych Dostawcy do świadczenia usługi wspierającej Krytyczne usługi biznesowe;
3. Udzielać Citi rozsądnej pomocy w celu umożliwienia Citi przeprowadzenia:
 - a. wszelkich wewnętrznych testów scenariuszy dotyczących zdolności Dostawcy do utrzymania się w granicach Tolerancji wpływu dla każdej Krytycznej usługi biznesowej w przypadku poważnego, ale prawdopodobnego zakłócenia działalności Citi lub działalności Dostawcy; a także
 - b. analizy wniosków z testów scenariuszy, które umożliwią Citi zidentyfikowanie słabych punktów i wszelkich działań niezbędnych do poprawy zdolności Dostawcy do skutecznego reagowania i przywracania sprawności po zakłóceniach w przyszłości.

Jeśli jakiegokolwiek wewnętrzne testy scenariuszy przeprowadzone przez Citi wykryją luki w zabezpieczeniach lub ograniczenia w zdolności Dostawcy do świadczenia usług w ramach odpowiedniej Tolerancji wpływu określonej przez Citi, a także po niewykonaniu przez Dostawcę jakiegokolwiek usługi w ramach odpowiedniej Tolerancji wpływu wyznaczonej przez Citi, strony uzgodnią plan (w tym harmonogram realizacji planu) zapewniający podjęcie przez Dostawcę kroków niezbędnych do usunięcia lub złagodzenia takich słabych punktów lub ograniczeń albo zaradzenia przyczynom niepozostawiania w granicach Tolerancji wpływu (jeśli dotyczy) tak szybko, jak to jest praktycznie możliwe.

14.15 Umowa powiernicza

Na żądanie Citi Dostawcy (i) udzielający Citi licencji na oprogramowanie do działania w środowisku Citi lub (ii) świadczący Usługę hostowaną Citi mają obowiązek zapewnić,

że Materiały depozytowe zostaną zdeponowane u wyznaczonego przez Citi powiernika, a także sporządzić harmonogram rejestracji deponenta lub inne formularze wymagane przez powiernika w odniesieniu do Materiałów depozytowych na mocy obowiązującej umowy powierniczej. Następnie, przez pozostały okres obowiązywania odpowiedniej umowy dotyczącej licencji lub Usługi hostowanej Dostawca będzie deponował zaktualizowane wersje Materiałów depozytowych u powiernika, zapewnić, że zdeponowany Kod źródłowy i inne Materiały depozytowe będą aktualne i zgodne z najnowszą wersją oprogramowania odpowiednią dla wersji oprogramowania lub Usług hostowanych wykorzystywanych przez Citi. Kod źródłowy lub inne aktualizacje Materiałów depozytowych zostaną dostarczone do powiernika w ciągu trzydziestu (30) dni od daty jakiegokolwiek aktualizacji oprogramowania licencjonowanego Citi lub modyfikacji Usług hostowanych przez Citi. Dostawca w pełni zastosuje się do wszystkich zobowiązań i wymogów deponenta określonych w umowie powierniczej. Dostawca ponosi wyłączną odpowiedzialność za wszelkie koszty i opłaty związane z powiernictwem, w tym m.in. opłaty za konfigurację, opłaty roczne, opłaty depozytowe, opłaty za usługi i wszelkie inne opłaty oraz koszty związane z powiernictwem. W przypadku Zdarzenia wydania depozytu Powiernik przekaze Materiały depozytowe Citi lub osobie wyznaczonej przez Citi, zgodnie z warunkami odnośnej umowy i umowy powierniczej.

W przypadku dostarczenia Kodu źródłowego (lub innych Materiałów depozytowych) do Citi lub osoby wyznaczonej przez Citi (bezpośrednio przez Dostawcę lub przez Powiernika w ramach wypełnienia zobowiązań wynikających z odpowiedniej umowy powierniczej) Kod źródłowy i Materiały depozytowe podlegają istniejącej licencji na mocy odpowiedniej umowy między Dostawcą a Citi; przy założeniu, że każda licencja zostanie uznana za uprawniającą Citi do korzystania i modyfikowania Kodu źródłowego i innych Materiałów depozytowych w sposób rozsądnie konieczny do: (i) zintegrowania zapewnienia zgodności oprogramowania i innych Materiałów depozytowych z Systemami Citi, (ii) zapewnienia zgodności oprogramowania lub innych Materiałów depozytowych z Obowiązującym prawem, standardami branżowymi lub praktyką rynkową, (iii) zapewnienia aktualności oprogramowania lub innych Materiałów depozytowych pod kątem wprowadzania innowacji technologicznych oraz (iv) zapewnienia, że oprogramowanie i inne Materiały depozytowe spełniają cele biznesowe Citi i jej Podmiotów stowarzyszonych w zakresie istniejącej Licencji. Wszelkie wersje Oprogramowania, które obejmują modyfikacje opracowane przez Citi lub w jej imieniu przy użyciu Kodu źródłowego, podlegają wszystkim postanowieniom niniejszej Części i odnośnej umowie; z zastrzeżeniem jednak, że Dostawca nie nabywa żadnych praw do modyfikacji, tytułu do modyfikacji ani udziału w modyfikacjach, a wszystkie prawa własności intelektualnej do tych modyfikacji przysługują wyłącznie Citi.

Dostawca wykorzysta komercyjnie uzasadnione rozwiązania w stosunku do stron trzecich, które dostarczyły oprogramowanie wykorzystywane w Oprogramowaniu, aby umożliwić Dostawcy umieszczenie kodu źródłowego takiego oprogramowania stron trzecich w Depozycie kodu źródłowego. Jeśli strona trzecia odmówi udzielenia Dostawcy tego prawa, Dostawca dołoży komercyjnie uzasadnionych starań, aby stosowna umowa o licencji na oprogramowanie strony trzeciej mogła zostać przeniesiona do Citi po wystąpieniu Zdarzenia wydania depozytu.

Kod źródłowy dostarczony Citi zgodnie z niniejszą Częścią będzie podlegał istniejącej Licencji na odpowiednie licencjonowane Oprogramowanie lub Usługi hostowane, *pod*

warunkiem że firma Citi będzie mogła korzystać z Kodu źródłowego i Oprogramowania w związku ze swoimi wymogami biznesowymi i operacyjnymi, aby zapewnić aktualność Oprogramowania pod kątem wprowadzania innowacji technologicznych i przestrzegać Obowiązującego prawa. Wszelkie wersje Oprogramowania, które obejmują modyfikacje opracowane przez Citi lub w jej imieniu przy użyciu Kodu źródłowego, podlegają wszystkim postanowieniom stosownej umowy; z zastrzeżeniem jednak, że Dostawca nie nabywa żadnych praw do modyfikacji, tytułu do modyfikacji ani udziału w modyfikacjach, a wszystkie Prawa własności intelektualnej do tych modyfikacji przysługują wyłącznie Citi.

15 GLOBALNE STANDARDY KONTROLI POD KĄTEM NIEKARALNOŚCI

Dotyczy wszystkich Dostawców zewnętrznych, którzy świadczą usługi na rzecz Citi.

15.1 Przegląd — Kontrola pod kątem niekaralności

Kontrola pod kątem niekaralności musi być przeprowadzana zgodnie z wszelkimi obowiązującymi przepisami prawa oraz regulacjami. Wszystkie opisane w niniejszym dokumencie informacje, w tym informacje własne, muszą zostać przekazane przez stosownych przedstawicieli Dostawcy, członków personelu i Podwykonawców Dostawcy. Zafałszowanie lub pominięcie informacji w życiorysie, podczas rozmowy rekrutacyjnej, w formularzu wdrażania lub podczas procesu wdrażania może stanowić podstawę do odmowy przydzielenia do zadania lub zakończenia udziału w jego realizacji zgodnie z przepisami miejscowego prawa, niezależnie od tego, kiedy takie zafałszowanie lub pominięcie zostanie wykryte. Nieprawidłowości zaistniałe podczas przeprowadzania kontroli mogą także stanowić podstawy do odmowy przydzielenia do realizacji zadania dla Citi lub zakończenia udziału w jego realizacji zgodnie z przepisami miejscowego prawa, niezależnie od tego, kiedy takie nieprawidłowości zostaną wykryte.

Dodatkowe informacje na temat przeprowadzania kontroli pod kątem niekaralności można znaleźć w dokumencie

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Gromadzenie podstawowych informacji oraz weryfikacja tożsamości

Zanim członek personelu Dostawcy rozpocznie realizację zadania na rzecz Citi, Dostawca musi zarejestrować jego imię i nazwisko, adres korespondencyjny i adres zamieszkania (jeśli są różne), numer telefonu oraz adres e-mail (w stosownych przypadkach). Personel Dostawcy musi także przedstawić dokumentację potwierdzającą tożsamość. Może to obejmować podanie informacji i/lub przedstawienie dokumentacji w postaci numeru PESEL, dowodu tożsamości ze zdjęciem wydanego przez organ rządowy lub paszportu.

15.3 Weryfikacja pod kątem sankcji

Cały personel Dostawcy, który wykonuje pracę w imieniu Citi, lub właściciel będący

w posiadaniu co najmniej 25% udziałów w firmie będącej Dostawcą Citi muszą także przedstawić dokumentację potwierdzającą tożsamość. Należy zweryfikować, czy żaden z członków personelu Dostawcy, co obejmuje Podwykonawców niezależnie od dostępu do danych/systemów/sieci Citi ORAZ/LUB dostępu do pomieszczeń Citi, nie figuruje na liście specjalnie wyznaczonych obywateli i osób zablokowanych (SDN, Specially Designated Nationals and Blocked Persons) Urzędu Kontroli Aktywów Zagranicznych (OFAC, Office of Foreign Assets Control) Departamentu Skarbu Stanów Zjednoczonych ani na liście regionów i jurysdykcji objętych sankcjami nakładanymi przez Stany Zjednoczone („Sankcje Stanów Zjednoczonych”), jak również na wszelkich listach oraz w odniesieniu do jurysdykcji objętych sankcjami nakładanymi przez organy spoza Stanów Zjednoczonych, w tym na skonsolidowanym wykazie transakcji finansowych Unii Europejskiej (UE), skonsolidowanym wykazie transakcji finansowych Rady Bezpieczeństwa ONZ (ONZ), wykazie podmiotów objętych sankcjami Wielkiej Brytanii (UK), jak również na listach publikowanych zgodnie z przepisami ustawowymi i wykonawczymi obowiązującymi w lokalnej jurysdykcji („Sankcje spoza Stanów Zjednoczonych”).

Listy OFAC są publicznie dostępne na następującej stronie internetowej: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Zgodność z prawem imigracyjnym

Dostawca musi wykazać, że utrzymuje i wdraża protokoły służące weryfikacji, że cały personel jest uprawniony do pracy w krajach, do których został przypisany. Ponadto Dostawca musi: (1) zapewnić, że cały personel jest uprawniony do pracy i (2) zachować zgodność ze wszystkimi obowiązującymi przepisami prawa, regulacjami oraz politykami (w tym wymogami w zakresie kwalifikowalności i weryfikacji uprawnień do zatrudnienia). Dostawca musi również wykazać, że dysponuje protokołami zapewniającymi zgodność jego personelu z przepisami i regulacjami prawa imigracyjnego oraz że utrzymuje takie protokoły, jak również że personel posiada odpowiedni status/rodzaj wizy do realizacji zadań i działań, do których został zaangażowany.

15.5 Historia zatrudnienia

Dostawcy są zobowiązani do weryfikacji historii zatrudnienia swojego personelu z ostatnich siedmiu (7) lub 10 lat, jeśli wymaga tego lokalne prawo. Historia zatrudnienia każdej osoby musi zostać zweryfikowana, aby zagwarantować, że pracodawcy, stanowiska, daty i wykonywane obowiązki zostały przedstawione zgodnie z prawdą. Członkowie personelu Dostawcy muszą także ujawnić fakt wcześniejszego zatrudnienia lub przydzielenia jako konsultant lub pracownik tymczasowy w Citi lub w jakiegokolwiek z jej spółek-poprzedników (w tym w szczególności: Citibank, Citicorp, Travelers, Salomon Brothers i/lub Smith Barney).

15.6 Wykształcenie

Dostawcy mają obowiązek zweryfikować najwyższy poziom wykształcenia osiągnięty przez jego personel. Zweryfikowane informacje powinny uwzględniać daty kształcenia, nazwy i adresy instytucji oraz uzyskane stopnie naukowe lub zawodowe.

15.7 Przeszłość kryminalna

Jeśli nie zabraniają tego przepisy prawa, pracownicy i podwykonawcy Dostawców mają obowiązek poinformować Citi, jeśli zostaną aresztowani, będą wezwani do stawienia się w sądzie, zostaną postawieni w stan oskarżenia lub będą skazani za jakiekolwiek przestępstwo, w tym przyznanie się do winy lub niepodważenie zarzutów, a także będą uczestniczyć w przedprocesowym postępowaniu mediacyjnym lub podobnym programie. Przed datą rozpoczęcia realizacji zlecenia przeprowadza się ocenę administracyjną pod kątem sprawdzenia wyroków sądowych i/lub pobrania odcisków palców, o ile jest to możliwe i dozwolone w świetle prawa. Wyroki sądowe za wykroczenia związane z kradzieżą, oszustwem, nieuczciwością lub naruszeniem zaufania lub też podobne wykroczenia określone inaczej w prawie lokalnym, z wyjątkiem sytuacji, w których przepisy prawa stanowią inaczej, mogą skutkować odmową i/lub niezakwalifikowaniem do realizacji zlecenia z Citi. Inne wyroki mogą skutkować odmową i/lub niezakwalifikowaniem do zawarcia umowy na podstawie obowiązującego prawa lokalnego i regulacji prawnych.

15.8 Ponowna kontrola

Jeśli członkowie personelu Dostawcy po zakończeniu realizacji zlecenia zostaną ponownie przydzieleni do Citi, muszą oni zostać poddani ponownej kontroli. Dodatkowe informacje na temat wymogów dotyczących ponownej kontroli można znaleźć w dokumencie

https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Transfery zagraniczne

Wszystkie kontrole muszą być przeprowadzane zgodnie z regulacjami kraju, w którym realizowane jest zlecenie. Jeśli członek personelu Dostawcy zostanie przeniesiony do innego kraju, daną osobę należy poddać ponownej kontroli zgodnie z wymogami danego kraju.

16 WYDATKI

Dostawcy, którym zgodnie z umową przysługuje prawo do ubiegania się o zwrot kosztów działalności gospodarczej.

16.1 Przegląd

Firma Citi zwróci wyłącznie uzasadnione koszty związane z działalnością biznesową, które zostały wcześniej przez nią zatwierdzone na piśmie i które Dostawca poniósł w związku z dostarczaniem Citi produktów lub świadczeniem usług na rzecz Citi, są zgodne z postanowieniami odpowiedniej Umowy lub, jeśli dotyczy, z Polityką Citi w zakresie zarządzania kosztami operacyjnymi oraz stosownymi Standardami i Procedurami, a także są odpowiednio udokumentowane potwierdzającymi rachunkami, fakturami, planami podróży lub innymi formami dokumentacji uznanymi przez Citi za akceptowalne.

16.2 Zwroty kosztów

Wydatki te należy odpowiednio udokumentować i należy na nie wystawi fakturę dla Citi zgodnie z wymogami Citi w zakresie fakturowania. Koszty Dostawcy nie mogą być ponoszone przez pracownika Citi w imieniu Dostawcy. Na fakturach przesyłanych Citi w celu uzyskania zwrotu kosztów w przypadku uzasadnionych i zatwierdzonych wydatków należy uwzględniać (oprócz wszystkich innych wymogów w zakresie fakturowania):

1. cel biznesowy wydatku;
2. kwotę i opis wydatku;
3. miejsce i datę wydatku;
4. nazwę/opis projektu, w ramach którego Dostawca świadczy usługi;
5. imiona i nazwiska oraz charakter relacji biznesowych przedstawicieli Citi zlecających usługi, w ramach których poniesiono dany wydatek; oraz
6. numer zlecenia zakupu, jeśli dotyczy.

W celu uzyskania informacji na temat dozwolonych zwrotów wydatków biznesowych należy skontaktować się ze stosowną główną osobą kontaktową w Citi. Wraz z wnioskiem o zwrot kosztów należy przedłożyć potwierdzające wydatek rachunki, faktury, plany podróży lub inne formy dokumentacji uznane za akceptowalne przez Citi. Wnioski o zwrot kosztów muszą być zgodne z postanowieniami odpowiedniej Umowy lub z Polityką Citi w zakresie zarządzania kosztami operacyjnymi oraz stosownymi Standardami i Procedurami Citi, a także zatwierdzone przez odpowiedniego sponsora biznesowego i/lub główną osobę do kontaktu w jednostce biznesowej Citi oraz zatwierdzone przez osobę, która została należycie upoważniona i dysponuje kwotą odpowiednią do danego towaru. Wydatki niezgodne z wytycznymi nie będą zwracane.

17 BEZPIECZEŃSTWO INFORMACJI (IS)

Dotyczy Dostawców, w tym Podwykonawców, którzy uzyskują dostęp do Informacji Citi, przetwarzają je, przechowują lub zarządzają nimi zgodnie z klauzulą tajności i definicją w Załączniku; lub hostują aplikacje z dostępem do Internetu pod marką Citi; lub mają dostęp do zasobów sieciowych Citi; lub wymagają dostępu bez nadzoru do obiektów Citi.

17.1 Przegląd

W niniejszej Części zawarto minimalne wymagania dla Dostawców Citi, w tym podwykonawców przetwarzających dane lub podwykonawców dostawców, którzy przechowują Informacje Citi, przetwarzają je, zarządzają nimi lub uzyskują do nich dostęp, hostują aplikacje Citi lub też mają połączenie sieciowe z Citi — w odniesieniu do oczekiwanych przez Citi mechanizmów kontroli ochrony informacji. Te wymogi gwarantują, że informacje są chronione zgodnie z obowiązującymi wymogami prawnymi i regulacyjnymi oraz najwyższymi standardami branżowymi (np. ISO/IEC 27001/2) w miejscach, w których firma Citi i jej Dostawcy prowadzą działalność. Jeśli w przepisach prawa miejscowego lub stosownych normach branżowych ustanowiono wyższe standardy niż podane w niniejszym dokumencie, Dostawcy muszą przestrzegać takich przepisów prawa lub norm. Ponadto od Dostawców może wymagać się wdrożenia dodatkowych praktyk i procedur w zakresie bezpieczeństwa informacji w ramach

przestrzegania przez Dostawców innych polityk Citi oraz postanowień i warunków umownych. Jeśli Dostawca zdecyduje się wdrożyć dodatkowe praktyki w zakresie bezpieczeństwa lub procedury związane z bezpieczeństwem informacji, Dostawca musi zadbać o to, aby takie praktyki i procedury nie stały w sprzeczności z minimalnymi środkami kontroli określonymi w niniejszym rozdziale.

17.2 Polityka bezpieczeństwa informacji i zarządzanie

Dostawcy muszą mieć udokumentowane polityki i standardy bezpieczeństwa informacji. Zarządzanie polityką musi obejmować jasno określony zakres ról i obowiązków oraz coroczny przegląd/aktualizację polityki i norm w celu zapewnienia zgodności z aktualnym stanem technologii, standardami branżowymi oraz wymogami prawnymi i regulacyjnymi.

17.3 Podział obowiązków

Dostawcy muszą dysponować procedurami zapewniającymi, że żadna osoba nie może wykonywać dwóch funkcji biznesowych lub dwóch funkcji IT lub dwóch funkcji w ramach Kontrolowanego Systemu Informatycznego z trwałym dostępem w przypadku tej samej czynności, zmiany, Systemu informatycznego lub transakcji bez upoważnienia lub wykrycia, chyba że istnieją odpowiednie środki kompensacyjne w celu ograniczenia ryzyka.

Tabela A

Funkcje	Opis funkcji
Opracowywanie/Inżynieria	Projektowanie, tworzenie lub modyfikowanie oprogramowania, sprzętu i konfiguracji; przykłady mogą obejmować: - Projektowanie i tworzenie nowego kodu aplikacji oraz powiązanych schematów baz danych - Produkty infrastruktury inżynierskiej i komponenty aplikacji - Dostosowywanie produktów technologicznych do integracji z oprogramowaniem oraz usługami
Zatwierdzanie	Zatwierdzanie przekazania zmian kodu do wdrożenia
Wdrażanie systemów / administrowanie systemami	Instalowanie, wdrażanie lub administrowanie oprogramowaniem, sprzętem oraz zmianami konfiguracji. Przykłady mogą obejmować: - Wykonywanie automatycznego lub ręcznego wdrożenia kodu do infrastruktury produkcyjnej - Instalowanie produktu technologicznego lub urządzenia

	- Uruchamianie lub zatrzymywanie usług w celu wsparcia rozwiązywania problemów oraz działań naprawczych w systemach z danymi produkcyjnymi
Przeglądanie aktywności identyfikatorów uprzywilejowanych	Weryfikacja działań związanych z zarządzaniem zmianami lub zdarzeń związanych z bezpieczeństwem systemu (np. ścieżek audytu)
Administrowanie identyfikatorami	Dodawanie, modyfikowanie i usuwanie identyfikatorów (Użytkownik, FID i Boty), uprawnień lub haseł
Funkcja biznesowa	Opis funkcji
Rozpoczynanie transakcji biznesowej	Inicjowanie (nazywane również wprowadzaniem, tworzeniem lub dokonywaniem) transakcji biznesowych i zmiana danych klientów
Zatwierdzanie transakcji biznesowych	Zatwierdzanie (nazywane również autoryzacją, sprawdzeniem lub dopuszczaniem) transakcji biznesowych
Funkcja IT	Opis funkcji
Operacje sieciowe	Zarządzanie urządzeniami i wsparcie operacyjne produktów zapewniających usługi infrastruktury sieciowej. Przykładami są routery sieciowe, przełączniki, zapory sieciowe i usługi nazw domen (DNS).
Operacje poza siecią	Zarządzanie urządzeniami i wsparcie operacyjne produktów, które nie zapewniają usług infrastruktury sieciowej. Przykładami są serwery, telefony i komputery.

17.4 Zaangażowanie kierownictwa w bezpieczeństwo informacji

Dostawcy, którzy będą oferować hosting aplikacji z dostępem do Internetu pod marką Citi i/lub będą mieli dostęp do Informacji Citi klasyfikowanych jako Poufne lub o wyższej klauzuli tajności, podlegają opracowanemu przez Citi Procesowi Oceny Bezpieczeństwa Informacji Posiadanych przez Osoby Trzecie (TPISA, Third Party Information Security Assessment), który ma na celu ocenę polityk, procedur i środków kontroli wdrażanych przez Dostawców i dotyczących przestrzegania wymagań Citi oraz wszelkich wymogów prawnych i/lub regulacyjnych (obowiązujących Citi lub Dostawców), które odnoszą się do bezpieczeństwa informacji.

Ocena składa się z kwestionariuszy wymagających od Dostawcy udzielenia odpowiedzi oraz dostarczenia dowodów pomocniczych i może obejmować wizyty w lokalizacjach Dostawcy, w których Informacje Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności są przechowywane, przetwarzane, zarządzane lub udostępniane przez stronę trzecią w celu sprostania potrzebom biznesowym firmy Citi i jej klientów. Ponadto Zespół ds. ciągłego monitorowania przez strony trzecie TPISA może monitorować Dostawcę za pomocą narzędzi do monitorowania cyberbezpieczeństwa, które wykorzystują publicznie dostępne informacje do identyfikacji podatnych na zagrożenia systemów, hostów, aplikacji i serwerów internetowych pod kątem oprogramowania nieotrzymującego już aktualizacji, otwartych portów podatnych na ataki, luk w zabezpieczeniach lub innych problemów. Jeśli wyniki procesu TPISA ujawnią lub wykażą kwestie związane z bezpieczeństwem, Citi udokumentuje takie wyniki w zawiadomieniu dla Dostawcy i będzie współpracować z Dostawcą nad ustaleniem rozwiązań takich problemów. Dostawcy muszą szybko wprowadzić konieczne rozwiązania i/lub dodać niezbędne kompensacyjne środki kontroli, aby odnieść się do obaw Citi wedle uznania Citi oraz zachować zgodność z terminami, tj. 180 dni kalendarzowych w odniesieniu do problemów związanych z wysokim ryzykiem, 240 dni kalendarzowych w odniesieniu do problemów związanych ze średnim ryzykiem i przed kolejnym terminem weryfikacji zgodności w przypadku problemów związanych z niskim ryzykiem, ponieważ takie problemy są oceniane przez Citi pod kątem ryzyka.

1. Dostawca musi regularnie przeprowadzać oceny swoich działań biznesowych i powiązanych środków kontroli pod kątem realizacji wdrożonych przez siebie standardów, polityk i procedur bezpieczeństwa informacji. Oceny okresowe muszą obejmować co najmniej:
 - a) Ocenę procesów wykorzystywanych przez Dostawcę w celu zapewnienia zgodności z polityką i standardami bezpieczeństwa informacji Dostawcy.
 - b) Ocenę zasobów pomocniczych, takich jak aplikacje i infrastruktura wykorzystywane przez Dostawcę oraz procesy dotyczące bezpieczeństwa informacji wykorzystywane przez podwykonawców Dostawcy (w stosownych przypadkach), które wspierają działania biznesowe Dostawcy lub umożliwiają Citi przeprowadzenie takich ocen. Zgodność jest wymagana, gdy strona trzecia podpisze nową umowę lub odnowi istniejącą umowę z podwykonawcą, który ma dostęp do Informacji Citi sklasyfikowanych przez Citi jako Poufne lub o wyższej klauzuli tajności, przetwarza je, zarządza nimi lub nimi dysponuje.
2. Kwestie wykryte w wyniku przeprowadzania wszelkich Ocen ryzyka Bezpieczeństwa Informacji (np. TPISA) należy udokumentować i monitorować aż do ich rozwiązania, jak również przekazać Citi dowody podjęcia działań naprawczych.
3. Jeśli dział Dostawcy odpowiedzialny za zarządzanie Bezpieczeństwem Informacji przenosi się poza granice kraju, Dostawca musi uzyskać na to udokumentowaną zgodę Citi.
4. Jeśli Dostawca dokonuje przejęcia nowego podmiotu, musi przeprowadzić dla przejętego podmiotu ocenę przestrzegania niniejszych Standardów.

5. Dostawca nie może oddelegowywać działań związanych z zarządzaniem bezpieczeństwem, w tym w szczególności zarządzania zaporą, zarządzania konfiguracjami bezpieczeństwa, zarządzania poprawkami ani Administrowania Bezpieczeństwem Informacji (ISA, Information Security Administration) w odniesieniu do systemów wykorzystywanych do przechowywania, przetwarzania i/lub przesyłania Informacji Citi, chyba że Citi wcześniej wyrazi na pisemną zgodę.
6. Jeśli Dostawca zajmuje się hostingiem oprogramowania lub witryny internetowej, która zawiera Informacje Citi lub oznaczenia Citi, należy przeprowadzać okresowe kontrole luk w zabezpieczeniach takiej witryny internetowej zgodnie z Wytycznymi Citi dotyczącymi Standardu Testowania Bezpieczeństwa Systemu (SSTS, System Security Testing Standard). Należy też rozwiązać wszelkie istotne problemy zidentyfikowane podczas takiej oceny w ramach czasowych określonych w tym Standardzie. Ponieważ standard SSTS nie jest zatwierdzony do dystrybucji zewnętrznej, Dostawcy muszą współpracować z Menedżerem ds. relacji Citi w celu zapewnienia zgodności z dokumentacją referencyjną. Ponadto Dostawca musi przestrzegać stosownych norm zarządzania Bezpieczeństwem informacji ISO/IEC 27001 (lub nowszych norm zarządzania bezpieczeństwem informacji, które ustanawiają wyższe standardy i protokoły) oraz postanowień w zakresie bezpieczeństwa informatycznego, zawartych w niniejszej Części (17).
7. Jeśli wymagana jest możliwość łączenia się z serwerami i/lub Systemami Informatycznymi w wewnętrznej sieci Citi, Dostawca ma obowiązek zawiadomić o tym przydzieloną główną osobę do kontaktu w jednostce biznesowej Citi, tak aby można było monitorować bieżący proces uzyskiwania połączenia.
8. Dostawca musi bezzwłocznie zawiadomić odpowiednią osobę do kontaktu w Citi (Właściciela Działów Biznesowych — BAO, Business Activity Owner) o każdym nieupoważnionym dostępie, przejęciu, utracie, uszkodzeniu lub usunięciu Informacji Citi oraz o wszelkich innych uszkodzeniach Systemów Informatycznych wykorzystywanych do przechowywania, przetwarzania i przesyłania Informacji Citi.
9. Dostawca musi dopilnować, aby wszystkie działania obarczone wysokim ryzykiem oraz zmiany danych wrażliwych miały ścieżki audytu umożliwiające przypisanie tych działań osobom, które je wykonały.
10. Dostawca musi dopilnować, aby wszystkie dane sklasyfikowane jako Poufne lub o wyższej klauzuli tajności były maskowane na ekranie i na papierze (co obejmuje np. raporty dotyczące monitorowania, wyjątków i przepisów oraz inne raporty).
11. Dostawca musi ograniczyć drukowanie, zapisywanie lub kopiowanie danych wrażliwych, w tym z zastosowaniem „urządzeń własnych”. Dostawca musi zwrócić lub usunąć wszystkie informacje Citi w uzgodnionym terminie w trakcie lub po zakończeniu umowy, chyba że przepisy prawa lub regulacje stanowią inaczej.
12. Dostawca ma obowiązek upewnić się, że cały personel Dostawcy (pracownicy, wykonawcy, pracownicy tymczasowi, podwykonawcy) mający dostęp do informacji Citi podpisał umowę o zachowaniu poufności.
13. Pracownicy Dostawcy muszą otrzymać podręcznik dla pracowników lub podobny dokument zawierający procedury dyscyplinarne w przypadku nieprzestrzegania kodeksu postępowania Dostawcy i polityki kadrowej, które to dokumenty muszą zostać przez nich potwierdzone w ramach procesu wdrożenia.

14. Dostawca musi mieć wdrożony proces odzyskiwania wszystkich aktywów na wypadek rozwiązania umowy o pracę lub rezygnacji pracownika albo osoby niebędącej pracownikiem.
15. Jeśli jakiegokolwiek Poufne informacje są utrzymywane lub w jakikolwiek sposób przechowywane w witrynie internetowej lub systemie dostępnym przez Internet, Dostawca musi ujawnić te informacje Citi. Ujawnienie to może być zawarte w opisie Usług. Jeśli Dostawca utrzymuje lub przechowuje Informacje poufne Citi, Dostawca przeprowadzi audyt SSAE 18 (lub inną miarodajną ocenę zatwierdzoną przez Citi) raz w roku w okresie obowiązywania niniejszej Umowy oraz przekaże Citi, nie mniej niż raz w roku, kopię raportów dokumentujących wyniki takiego audytu SSAE 18 lub jakiegokolwiek miarodajnej oceny zatwierdzonej przez Citi.
16. Jeśli Dostawca zostanie przejęty lub przejmie inny podmiot w ramach fuzji, przejęcia lub podobnej transakcji, a taka transakcja może mieć wpływ na Usługi, Dostawca musi o tym niezwłocznie i pisemnie powiadomić Citi, a Dostawca musi przeprowadzić ocenę bezpieczeństwa informacji w powstałym podmiocie zgodnie z niniejszymi Wymaganiami, aby zapewnić, że takie przejęcie lub taka fuzja nie wpłynie na zgodność z Wymaganiami.

17.5 Ryzyko dotyczące bezpieczeństwa informacji Podwykonawcy

Dostawca musi wymagać, aby podwykonawcy mający dostęp do danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności wymagali przed zawarciem umowy i okresowo po jej zawarciu przeprowadzania oceny Bezpieczeństwa informacji (IS) przez wykwalifikowany personel ds. bezpieczeństwa informacji. Oceny te należy przeprowadzać zgodnie z zatwierdzonym przez kierownictwo procesem obejmującym wszystkie etapy procesu oceny od rozpoczęcia do zarządzania problemami. Ocena bezpieczeństwa informacji podwykonawcy powinna obejmować kwestionariusz lub równoważne narzędzie do oceny stanowiska podwykonawcy w dziedzinie bezpieczeństwa informacji zgodnej z dziedzinami uwzględnionymi w kwestionariuszu oceny bezpieczeństwa informacji Citi (TPAQ, Third Party IS Assessment Questionnaire). Ocena powinna zawierać logiczną metodę obliczania ryzyka związanego z bezpieczeństwem informacji związanego z zaangażowaniem podwykonawcy. Dostawca ma obowiązek monitorowania ukończenia oceny oraz zarządzania zaobserwowanymi problemami i planami działań naprawczych aż do ich zakończenia.

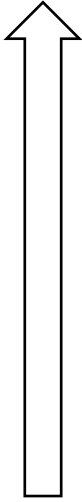
17.6 Odpowiedzialność za zasoby

1. Dostawca musi zadbać o prowadzenie ewidencji całego sprzętu i wszystkich aplikacji pozostających pod jego kontrolą, które są wykorzystywane do przechowywania, przetwarzania lub przesyłania Informacji Citi.
2. Dostawca musi też zadbać o to, aby pod jego kontrolą prowadzono ewidencję zasobów będących Informacjami Citi zgodnie z procesem stosowanym w celu właściwego utrzymania dokładności i kompletności tej ewidencji.
3. Dostawca musi odpowiadać za ochronę wszystkich Informacji Citi pozostających pod jego kontrolą.
4. Dostawca jest odpowiedzialny za działania swoich użytkowników w sposób zgodny z praktyką branżową.

5. Niezbędne jest uniemożliwienie dostępu Użytkownika do osobistych zewnętrznych kont e-mail i systemów przechowywania danych w chmurze z poziomu globalnej sieci Dostawcy, w której znajdują się Informacje Citi.

17.7 Klasyfikacja informacji i postępowanie z nimi.

Citi klasyfikuje informacje zgodnie z poniższą tabelą Klasyfikacją Informacji: W Załączniku znajdują się definicje i przykłady każdej klasyfikacji informacji wymienionej poniżej.

ZASTRZEŻONE	Najbardziej wrażliwe
WRAŻLIWE INFORMACJE UMOŻLIWIAJĄCE USTALENIE TOŻSAMOŚCI	
INFORMACJE POUFNE UMOŻLIWIAJĄCE USTALENIE TOŻSAMOŚCI	
POUFNE	
INFORMACJE WEWNĘTRZNE UMOŻLIWIAJĄCE USTALENIE TOŻSAMOŚCI	
WEWNĘTRZNE	
PUBLICZNE	Najmniej wrażliwe

1. Bazując na klasyfikacji Informacji Citi, Citi musi współpracować z Dostawcą w celu określenia poziomu zabezpieczeń wymaganych do ochrony takich informacji, a Dostawca musi zapewnić wdrożenie odpowiednich środków kontroli, wraz z wszelkimi dodatkowymi lub zmodyfikowanymi poziomami zabezpieczeń, których Citi może wymagać.
2. Informacje sklasyfikowane jako Wewnętrzne lub o wyższej klauzuli tajności muszą być przechowywane na urządzeniach zarządzanych przez strony trzecie, które podlegają umowie podpisanej między Stroną Trzecią a Citi, zawierającej zgodne z zasadami i standardami Citi postanowienia dotyczące poufności.
3. Jeśli Dostawca zezwala na korzystanie z urządzeń do przechowywania danych Citi niebędących własnością firmy (tj. urządzeń zarządzanych przez stronę czwartą), musi wdrożyć politykę, która wymaga specjalnej zgody kierownictwa oraz ustanowić wytyczne i procedury monitorowania dotyczące korzystania z Informacji Citi i ich usuwania.
4. Dostawca musi zawsze chronić Informacje Citi przed nieupoważnionym dostępem, modyfikacjami lub usunięciem.
5. Informacje Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności, przesyłane za pośrednictwem Przenośnych nośników elektronicznych (ETM, Electronic Transportable Media) muszą być szyfrowane przy użyciu

zatwierdzonego algorytmu kryptograficznego. Konieczne jest też potwierdzenie odbioru. Dostawca musi potwierdzić, że zamierzony odbiorca otrzymał ETM w przewidywanym terminie dostawy. Jeśli Dostawca nie otrzyma potwierdzenia otrzymania w przewidywanym terminie dostawy, musi zawiadomić Citi o tym fakcie.

17.8 Bezpieczna konfiguracja

1. Dostawca zobowiązany jest do utrzymywania udokumentowanych standardów bezpiecznej konfiguracji wszystkich aktywów, które mogą być wykorzystywane do przechowywania, przetwarzania, uzyskiwania dostępu lub przekazywania Informacji Citi.
2. Dostawca musi wdrożyć środki kontroli w zakresie bezpieczeństwa informacji do swoich procesów i procedur dotyczących wyboru, rozwoju i wdrażania aplikacji, produktów i usług.
3. Dostawca musi zapewnić procedurę bezpiecznej kompilacji dla wszystkich systemów, w których przechowywane, przetwarzane i/lub przesyłane są Informacje Citi.
4. Dostawca musi utrzymywać bezpieczny obraz lub szablon dla wszystkich systemów.
5. Wszystkie domyślne konta użytkowników i hasła muszą być zmieniane i/lub usuwane z systemów, urządzeń sieciowych i aplikacji wspieranych przez sprzedawców.
6. Każdy system lub usługa, która została naruszona, musi zostać odtworzona i skonfigurowana przy użyciu obrazu lub szablonu, który ma sprawdzoną integralność.
7. Każda zmiana, która ma zostać wprowadzona do bezpiecznej konfiguracji, musi zostać zatwierdzona przez kierownictwo w ramach procesu Dostawcy dotyczącego zarządzania zmianami.
8. Dostawca musi powiadomić Citi o wszelkich zmianach wprowadzonych względem bezpiecznej konfiguracji.
9. Procedura bezpiecznej kompilacji musi obejmować narzędzia wspierające automatyczne sprawdzanie konfiguracji ustawień bezpieczeństwa / standardowej kompilacji w momencie wdrożenia produkcji oraz bieżące monitorowanie zgodności z konfiguracją bazową i odchyłeń od niej.

17.9 Wymagania dotyczące szyfrowania

Dostawca nie może przekazywać informacji sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności w sposób nieszyfrowany. Informacje sklasyfikowane jako Poufne lub o wyższej klauzuli tajności muszą być **kompleksowo** szyfrowane za pomocą narzędzi lub rozwiązań zatwierdzonych przez Citi. Zatwierdzone protokoły i odpowiednie numery wersji szyfrowanych transmisji danych są następujące:

1. Podczas wymiany informacji dotyczących uwierzytelniania i autoryzacji: SAML v2.0, OAuth v2.0 (tylko autoryzacja);
2. W celu ochrony kanałów komunikacji i powiązanej wymiany kluczy dozwolone są tylko następujące protokoły bezpieczeństwa sieci:
 - a) TLS v1.3 to protokół preferowany — dozwolone są wszystkie pakiety TLS v1.3. Jeśli protokół TLS 1.3 jest jedynym włączonym protokołem,

- nie jest konieczna dodatkowa weryfikacja.
- b) Jeśli protokół TLS v1.3 nie jest technicznie możliwy do zastosowania i wykorzystywany jest protokół TLS 1.2, ocena B lub wyższa od SSLabs jest obecnie akceptowalna i nie jest konieczna dodatkowa weryfikacja.

Dane stale przechowywane w środowisku zewnętrznym Strony trzeciej zatwierdzonej przez Citi lub podczas wymiany muszą być w pełni zaszyfrowane przy użyciu zatwierdzonych przez Citi narzędzi i rozwiązań. Zatwierdzone algorytmy i długości kluczy używanych do szyfrowania danych są następujące:

1. **Zaawansowany standard szyfrowania (AES, Advanced Encryption Standard):** Zatwierdzone długości kluczy: co najmniej 256 bitów. Tryby ograniczone: Tryb elektronicznej książki kodowej (EBC, Electronic Codebook) jest zabroniony, chyba że ilość zwykłego tekstu jest mniejsza lub równa długości bloku. Szyfrowanie dysku: Wymagany jest algorytm AES z kluczem 256-bitowym. Algorytm AES z kluczem o długości 128 bitów jest dozwolony jako opcja szyfrowania TLS; do dnia 31 grudnia 2028 r. będą one jednak wycofane na rzecz szyfrowania o sile 256 bitów lub wyższej, aby umożliwić dostosowanie Citi do międzynarodowych ram czasowych (Ref, NIST 8547 IPD).
2. **ChaCha20 (szyfr strumieniowy dla powiązanych przypadków użycia):** Zatwierdzone długości kluczy: 128 lub 256 bitów, z 96-bitowym identyfikatorem jednorazowym i blokiem 32-bitowym lub 64-bitowym identyfikatorem jednorazowym i blokiem 64-bitowym. Maksymalny rozmiar danych: 16 petabajtów.

Zatwierdzone systemy kryptograficzne klucza publicznego, wymiana kluczy, mechanizmy uzgadniania, skrót wiadomości i funkcje wyprowadzania klucza są następujące:

Powiadomienie dotyczące Gotowości kwantowej Dostawcy: Dostawcy są zobowiązani przedstawić swój plan dotyczący zakresu ujętego w *tabeli 2* i *tabeli 4* dokumentu NIST IR 8547 (ipd) zespołowi ds. Programu gotowości kwantowej Citi za pośrednictwem ([łącze do ankiety](#)).

1. **Kryptosystemy z kluczem publicznym i minimalne długości kluczy:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 bitów.
 - b) Digital Signature Algorithm (DSA): 2048 bitów. Algorytmu DSA nie wolno używać do zabezpieczania danych Citi przetwarzanych lub przechowywanych poza Citi.
 - c) Elliptic Curve Digital Signature Algorithm (ECDSA): 256 bitów i zgodnie z normą ANSI X9.62 z krzywymi zalecanymi przez NIST.
2. **Mechanizmy wymiany i uzgadniania kluczy oraz minimalne długości kluczy:**
 - a) Diffie-Hellman (DH) / Ephemeral Diffie-Hellman (DHE): 2048 bitów.
 - b) Elliptic-curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE): 256 bitów i zgodnie z normą ANSI X9.63 z krzywymi zalecanymi przez NIST¹.

¹ Preferowany jest algorytm ECDHE.

3. **Funkcje skrótu wiadomości:** Tworzenie klucza szyfrującego o długości większej niż liczba losowych bitów w materiale użytym do wygenerowania skrótu jest zabronione.
 - a) SHA-1: Akceptowane w przypadku aplikacji z podpisami innymi niż cyfrowe. Rodzina SHA-2, rodzina SHA-3 i POLY-1305: Dopuszczalne dla wszystkich zastosowań funkcji skrótu kryptograficznego.
4. **Funkcje wyprowadzania kluczy na podstawie hasła i minimalne wymagania:**
 - a) PBKDF2: Minimalna liczba iteracji wynosząca 10 000 z solą o długości co najmniej 16 bajtów.
 - b) HKDF: Musi być z solą i musi być uwzględniona wartość wejściowa informacji.
 - c) SCRYPT: Minimalna liczba rund / współczynnik kosztu 10.
 - d) Stosowanie algorytmu NIST SP800-108 KDF do szyfrowania strumienia jest zabronione. Dopuszczalne są tryby KDF NIST SP 800-108, tj. tryby licznika, sprzężenia zwrotnego i iteracji dwupotokowej.
 - e) Zalecane jest stosowanie Argon2.
5. **Funkcje skrótu hasła i minimalne wymagania:**
 - a) Bcrypt (do lokalnego przechowywania danych uwierzytelniających): Minimalna liczba rund / współczynnik kosztu co najmniej 10.
 - b) Zalecane jest stosowanie Argon2 lub PBKDF2 do hashowania haseł w przypadku ich lokalnego przechowywania w środowiskach lub systemach wdrożonych u Dostawcy.

17.10 Zewnętrzny adres e-mail

Wymóg szyfrowania indywidualnych wiadomości e-mail zawierających Informacje Citi, sklasyfikowane przez Citi jako Poufne lub o wyższej klauzuli tajności, względem których Dostawca nie może stosować zatwierdzonego przez Citi oprogramowania dla użytkowników końcowych (ani takich narzędzi) ze względu na przepisy lub politykę współpracy z Dostawcami, można spełnić poprzez szyfrowanie podczas przesyłania danych (np. szyfrowanie bramka-bramka z użyciem protokołu TLS (Transport Layer Security)). Zatwierdzone bezpieczne protokoły do szyfrowania wiadomości e-mail:

1. **Protokół IBE (Identify-Based Encryption)** oferuje szyfrowanie wiadomości e-mail i może być używany wyłącznie w ramach rozwiązań Citi przeznaczonych dla klientów oraz w bezpiecznych systemach obsługi poczty elektronicznej oraz eDelivery.
2. Funkcja **Mandatory TLS (MTLS)** umożliwia szyfrowanie sesji (nie szyfruje zawartości wiadomości e-mail) i może być wykorzystywana przez dostawców, partnerów i klientów, którzy wcześniej wynegocjowali warunki korzystania z tej funkcji.
3. **Funkcja DKIM (Domain Keys Identified Mail)** umożliwia uwierzytelnianie źródeł i zarządzanie kluczami oraz jest przeznaczona do użytku z dostawcami, partnerami i klientami.

17.11 Sieci prywatne

Sieci prywatne podlegające niezależnej regulacji uznanego organu i spełniające standardy sektora usług finansowych w zakresie dokonywania transakcji między

licencjonowanymi lub akredytowanymi kontrahentami (np. SWIFT lub bank centralny) można uznać za zwolnione z wymogów dotyczących Informacji poufnych umożliwiających ustalenie tożsamości podczas przesyłania do czasu, aż sieci takie będą mogły zapewnić odpowiednią infrastrukturę w pełni obsługującą przesyłanie szyfrowanych danych.

17.12 Połączenia głosowe i faks

Informacje sklasyfikowane przez Citi jako Poufne lub o wyższej klauzuli tajności, które są przesyłane faksem lub omawiane głosowo (w tym poprzez Voice Over IP (VOIP)), można przysyłać bez szyfrowania. Jeżeli będzie to konieczne, Dostawca musi opracować konkretne procedury oraz wytyczne do ochrony informacji o statusie Poufne lub o wyższej klauzuli tajności, przesyłanych tymi kanałami.

17.13 Zarządzanie kluczami i certyfikatami kryptograficznymi

Termin „bezpieczna granica” używany w tej części odnosi się do programów walidacji modułów kryptograficznych (CMVP, Cryptographic Module Validation Program), takich jak Federalny standard ochrony informacji (FIPS, Federal Information Protection Standard), zweryfikowanej granicy (minimalnym akceptowalnym poziomem bezpieczeństwa jest poziom 2 wg standardu FIPS 140-2/3). (Dopuszczalne są poufne enklawy obliczeniowe, takie jak enklawy AWS Nitro. Inne wyjątkowe przypadki granic bezpieczeństwa muszą zostać zatwierdzone przez Citi).

1. Dostawca musi przestrzegać aktualnych norm branżowych dotyczących algorytmów szyfrowania i minimalnych długości kluczy używanych do szyfrowania i podpisywania (włączając w to klucze SSH). Gdy takie algorytmy i długości kluczy są aktualizowane w celu dostosowania się do standardów branżowych, Dostawca musi to realizować zgodnie ze swoim Procesem zarządzania zmianami.
2. Dostawca musi mieć formalnie udokumentowany proces cyklu życia zarządzania kluczami, kodami dostępu i certyfikatami z wdrożonymi mechanizmami, które zabezpieczają wrażliwe dane przed nieautoryzowanym użyciem lub ujawnieniem. Wszystkie tajne dane kryptograficzne i zdarzenia związane z cyklem życia kluczy muszą być realizowane wyłącznie w bezpiecznym środowisku. Każdy dostęp do uprzywilejowanych i bezpiecznych granic musi być udokumentowany. Dostawca musi przedstawić diagram sekwencji wszystkich kluczowych zdarzeń w cyklu życia, podkreślający zaangażowane podmioty i granice.
3. Klucze kryptograficzne muszą mieć unikatowy cel i nigdy nie mogą być używane do żadnych innych celów, takich jak użycie tego samego klucza szyfrującego zarówno do szyfrowania dysków, jak i szyfrowania danych, albo użycie tego samego klucza szyfrującego zarówno do szyfrowania obciążenia, jak i szyfrowania bazy danych. Ponowne wykorzystywanie kluczy kryptograficznych w wielu klientach przez dostawcę SaaS jest domyślnie zabronione i może być dozwolone wyłącznie w przypadkach użycia o niskim ryzyku i niekrytycznych, obejmujących informacje Citi o klauzuli poufności poniżej kategorii Poufne informacje umożliwiające ustalenie tożsamości, Wrażliwe informacje umożliwiające ustalenie tożsamości i Zastrzeżone, pod warunkiem uzyskania wyraźnej zgody Rady Architektury Bezpieczeństwa (SAC, Security Architecture Council).

4. W przypadku wszystkich kluczy kryptograficznych (symetrycznych i asymetrycznych) klucza prywatnego ani materiałów klucza prywatnego (takich jak nasiona lub część klucza prywatnego) nie można w żadnym momencie wyświetlać w formie tekstu jawnego. Klucz prywatny lub materiały klucza prywatnego (takie jak nasiona i części klucza prywatnego) nigdy nie mogą przekraczać bezpiecznej granicy — z wyjątkiem kluczy efemerycznych, takich jak klucze sesji dynamicznych. Jeśli rozwiązanie wymaga wyprowadzenia klucza symetrycznego, klucza prywatnego lub przesłania materiałów klucza prywatnego między bezpiecznymi enklawami/granicami dostępu uprzywilejowanego, muszą one być przesyłane wyłącznie w postaci zaszyfrowanej przy użyciu klucza symetrycznego (Symmetric Key Wrapping Key) lub klucza publicznego (Public Key Transport Key) wyłącznie za pośrednictwem wzajemnie szyfrowanych tuneli TLS, a powiadomienie o takiej potrzebie musi zostać pisemnie zatwierdzone przez Citi. W takich przypadkach klucz Private Key Transport Key nie może nigdy przekroczyć bezpiecznej granicy dostępu uprzywilejowanego, w obrębie której został wygenerowany.
5. Klucz Symmetric Key Wrapping musi być podzielony na co najmniej dwa składniki klucza, a przed dystrybucją oraz ręcznym wprowadzaniem/ladowaniem klucza musi być szyfrowany metodą XOR. Klucz Symmetric Key Wrapping Key musi mieć wewnątrz bezpiecznej granicy skojarzone odpowiednie listy kontroli dostępu (ACL), takie jak moduły zatwierdzone przez CMVP. Nie może także nigdy być przechowywane poza obszarem objętym bezpieczną granicą.
6. Dostęp człowieka, usługi lub automatycznego agenta do magazynów kluczy lub bezpiecznych granic obejmujących klucze prywatne, kody dostępu lub materiały kluczy prywatnych (takie jak nasiona lub części klucza prywatnego) musi być odpowiednio segregowany i wyposażony w środki kontroli ograniczające dostęp wyłącznie do upoważnionych osób lub systemów.
7. Każde żądanie dostępu do magazynów kluczy zawierających klucze prywatne lub symetryczne musi być rejestrowane i dokumentowane z uwzględnieniem takich szczegółowych informacji, jak: kto, kiedy i cel dostępu, do celów audytu.
8. Dostawca nie może używać certyfikatów z podpisem własnym, certyfikatów z symbolami wieloznacznymi ani domyślnych certyfikatów SSL.
9. Klucze kryptograficzne muszą mieć określony przedział czasu szyfrowania, jak sugerowano w przepisach NIST SP800-57, część 1, wersja 6. Klucze muszą być zmieniane lub stosowane rotacyjnie przed wygaśnięciem ich terminu ważności, aby uwzględnić okresy zmian, konflikty w harmonogramie i zawieszanie się systemu.
 - a) Podczas wymiany wygasłego certyfikatu ponowne wykorzystanie starej asymetrycznej pary kluczy jest zabronione.
10. Klucze kryptograficzne należy traktować jako naruszone w momencie, gdy istnieje podejrzenie, że integralność klucza, nośnik, na którym klucz jest przechowywany lub udostępniany, lub poufność klucza symetrycznego lub prywatnego zostały naruszone. Wszystkie naruszone klucze muszą zostać usunięte z użytku, a wszystkie odpowiednie certyfikaty muszą zostać odwołane.

11. Sieci bezprzewodowe muszą być szyfrowane z zastosowaniem algorytmów szyfrowania spełniających normy branżowe.
12. Dostawcy korzystający z jakichkolwiek mechanizmów szyfrowania muszą stosować narzędzia i techniki zarządzania kluczami, które spełniają normy branżowe. Role zarządzania kluczami muszą być oddzielone od zarządzania operacyjnego.
13. Dostawcy mogą korzystać z natywnych w chmurze usług KMS i PKI tylko w przypadku, gdy zapewniona jest ich interoperacyjność z usługami PKI i KMS dostarczonymi przez Usługi zabezpieczania danych Citi, a kontrola kryptograficzna nie jest przekazywana poza zarządzanie kryptograficzne Citi.

17.14 Odpowiedzialność za kontrolę dostępu

Dostawca odpowiada za ochronę wszystkich Kontrolowanych Systemów Informatycznych, które są wykorzystywane do przechowywania, uzyskiwania dostępu, zarządzania, przetwarzania i/lub przesyłania Informacji Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności, przed nieupoważnionym dostępem. Ponadto, dostawca odpowiada za egzekwowanie zasady najmniejszych przywilejów poprzez ograniczanie uprawnień użytkowników do minimalnego poziomu dostępu wymaganego dla każdego stanowiska oraz poprzez zapewnianie rozsądnego dostępu do wszystkich systemów i aplikacji. Środki kontroli muszą być w pełni udokumentowane i możliwe do skontrolowania. Nadawanie i odbieranie dostępu, w tym resetowanie haseł i ich włączanie, musi odbywać się za pomocą zautomatyzowanego procesu zawsze, gdy to możliwe, aby zminimalizować ryzyko potencjalnego błędu ludzkiego spowodowanego przyznaniem zbyt szerokiego zakresu uprawnień oraz w celu zapewnienia zgodności ze standardami branżowymi.

1. Dostawca jest odpowiedzialny za prawa dostępu wszystkich użytkowników w swojej organizacji.
2. Dostawca musi wdrożyć środki kontroli dostępu gwarantujące, że użytkownikom będą przyznawane wyłącznie uprawnienia ściśle konieczne do pełnienia ich funkcji.
3. Dostawca musi wdrożyć proces gwarantujący, że usunięto, wyłączono lub obłożono ochroną wszelkie domyślne możliwości dostępu. Pozwoli to zapobiec nieupoważnionemu dostępowi.

17.15 Zarządzanie dostępem użytkowników

Dostawca musi zarządzać zapewnianiem logicznego dostępu do systemów i aplikacji, które przetwarzają, przechowują i/lub przekazują Informacje Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności. Obejmuje to:

1. Identyfikację i inwentaryzowanie zatwierdzonych systemów uwierzytelniania.
2. Wymogiem jest, aby każdy dostęp do danych Citi wymagał zatwierdzenia przez kierownika lub osobę przez niego wyznaczoną oraz właściciela systemu. Dostawca ma obowiązek dopilnować, aby wszyscy członkowie jego personelu mający dostęp do danych Citi uzyskali taki dostęp zgodnie z zasadą ograniczonego dostępu.

3. Wymóg, aby łączenie uprawnień/funkcji nie było możliwe dla użytkowników indywidualnych ze względu na wynikowe konflikty interesów lub naruszenie zasady weryfikacji czworga oczu (maker-checker).
4. Proces monitorowania mający na celu nadzorowanie przyznawania praw dostępu każdemu użytkownikowi w systemie lub unieważniania takich praw oraz zarządzanie nimi.
5. Wnioski o dostęp nie mogą polegać na dublowaniu/klonowaniu uprawnień innego użytkownika; wnioski powinny określać konkretne role/uprawnienia wraz z uzasadnieniem biznesowym, aby zapobiec rozszerzaniu uprawnień i wymuszać zasadę minimalnych uprawnień.

17.16 Identyfikacja i uwierzytelnianie użytkownika

Wszystkie Systemy informatyczne kontrolowane przez Dostawcę muszą uwierzytelniać tożsamość użytkowników lub systemów uzyskujących dostęp do tych platform przed rozpoczęciem sesji lub transakcji, w której uzyskiwany jest dostęp do Informacji Citi.

1. Użytkownicy muszą przejść indywidualną identyfikację lub zostać dopasowani do platform technologicznych poprzez identyfikator Użytkownika.
2. Użytkownicy muszą zostać uwierzytelnieni na platformie technologicznej wykorzystującej zatwierdzoną metodę uwierzytelniania. Dostawca powinien skontaktować się z Właścicielem Działów Biznesowych (BAO), aby poznać obecnie dopuszczalne sposoby.
3. Każdy przypadek użytkowania udostępnionej infrastruktury uwierzytelniającej (np. jednorazowa rejestracja, rejestracja w ograniczonym zakresie lub inne udostępnione usługi uwierzytelniania) musi być zgodny z wymogami uwierzytelniania Citi; Dostawca powinien skontaktować się z głównym Właścicielem Działów Biznesowych w jednostce biznesowej Citi, aby poznać aktualnie aprobowane sposoby.
4. Podczas przesyłania i przechowywania należy szyfrować dane umożliwiające weryfikację tożsamości (IVD, Identify Verification Data), które są wykorzystywane do uwierzytelniania użytkownika w Systemie Informatycznym. Wymagania dotyczące szyfrowania znajdują się w punkcie 17.9.
5. Każde konto używane przez personel Dostawcy w celu uzyskania dostępu do systemów Citi musi być przypisane do unikatowego identyfikatora nadanego przez Citi (np. GEID); w celu zapewnienia identyfikowalności, egzekwowania SOD i gotowości do audytu zabrania się używania ogólnych/współdzielonych identyfikatorów użytkowników (osób).

17.17 Identyfikacja dostępu uprzywilejowanego i tymczasowy dostęp uprzywilejowany

Dostawca musi utrzymywać wykaz wszystkich tożsamości i identyfikować osoby mające dostęp uprzywilejowany lub dostęp do repozytoriów elektronicznych (zbiorów danych lub baz danych obsługujących aplikacje biznesowe), które zawierają informacje sklasyfikowane jako Informacje poufne umożliwiające ustalenie tożsamości lub o wyższej klauzuli tajności. Dostawca musi wdrożyć środki kontroli chroniące przed

nieupoważnionym wykorzystaniem tych Tożsamości. Jeśli pracownik wymaga dostępu do uprzywilejowanego identyfikatora lub do wspomnianych wcześniej repozytoriów elektronicznych, dostęp ten musi zostać przyznany w ramach tymczasowych procesów zarządzania dostępem, które:

1. Wymagają, by wnioskodawca znajdował się na wstępnie zatwierdzonej liście upoważnionych użytkowników lub uzyskał zgodę w momencie użytkowania Systemu;
2. Wymagają udokumentowanego uzasadnienia w zgłoszeniu dotyczącym zmiany/problemu przed przyznaniem dostępu;
3. Obejmują niezależną ocenę działań prowadzonych po udzieleniu dostępu;
4. Obejmują proces inicjowania odwołania/usunięcia dostępu po zakończeniu tymczasowego okresu przyznania dostępu.
5. Umożliwiają przedłużenie dostępu do produkcji i stabilizacji po wdrożeniu, np. po znaczącej modernizacji lub usunięciu awarii / naprawie, do siedmiu (7) dni kalendarzowych.

17.18 Weryfikacja praw dostępu użytkownika

1. Dostawca musi wdrożyć udokumentowany proces przeglądu, weryfikacji i usuwania zbędnych uprawnień użytkownika w Kontrolowanych Systemach Informatycznych wykorzystywanych do przechowywania, przetwarzania, przesyłania Informacji Citi i/lub zarządzania nimi — co najmniej raz na pół roku.
2. Użytkownicy nie mogą sprawdzać ani zatwierdzać własnych uprawnień ani uprawnień osoby, która przeniosła na nich obowiązek sprawdzania uprawnień.
3. Po zmianie stanowiska przez pracownika Dostawcy w ramach Citi Dostawca ma 14 dni kalendarzowych na przejrzanie dostępu i uprawnień oraz usunięcie dostępu do danych Citi, jeśli nie jest on już wymagany na nowym stanowisku pracownika.

17.19 Procedury bezpiecznego logowania

1. Zablokowane identyfikatory logowania użytkowników należy ponownie aktywować poprzez zgodną ze standardami branżowymi usługę resetowania lub inną autoryzowaną funkcję. Tekst baneru, jeśli jest obsługiwany przez system operacyjny lub aplikację, musi być wyświetlany we wszystkich punktach dostępu do sieci, w których użytkownik wstępnie się loguje lub przechodzi uwierzytelnianie.

17.20 System zarządzania hasłami

1. Hasła statyczne Użytkowników nie mogą być nigdy wyświetlane na ekranie w formie wyraźnego tekstu. Wymóg ten nie dotyczy funkcji przełączania widoczności hasła, pod warunkiem że:
 - (1) wpisywane hasło jest domyślnie maskowane,
 - (2) widoczność hasła może być inicjowana tylko przez wyraźne działanie użytkownika,
 - (3) hasło jest automatycznie ponownie maskowane w ciągu maksymalnie 15 sekund po zakończeniu działania użytkownika.

2. Hasła identyfikatorów funkcji uprzywilejowanych nie mogą być zakodowane na stałe w postaci wyraźnego tekstu.
3. Hasła statyczne muszą składać się z co najmniej dziesięciu (10) znaków, które muszą zawierać litery i cyfry oraz uwzględniać wielkość liter. Rozróżnianie wielkości liter w hasłach statycznych musi zostać sprawdzone w każdym punkcie uwierzytelniania. Hasła stałe Identyfikatorów funkcjonalnych (FID) muszą zawierać co najmniej 15 znaków w aplikacjach wprowadzonych po 31 sierpnia 2026 r.
4. Wykorzystywanie numerów PIN jako jedyne sposoby uwierzytelniania w celu uzyskania dostępu do Systemów informatycznych możliwe jest wyłącznie wtedy, gdy takie numery PIN są niezbędne ze względu na ograniczenia fizyczne urządzeń (np. klawiatura numeryczna, telefon, karta chipowa).
5. Wszystkie hasła statyczne należy zmieniać co najmniej co 90 dni kalendarzowych.
6. Wszystkie hasła statyczne należy zablokować po nie więcej niż sześciu (6) kolejnych nieudanych próbach logowania lub sześciu (6) kolejnych próbach resetowania hasła. Hasła muszą być odblokowywane za pomocą funkcji administratora identyfikatora lub odblokowywane automatycznie po co najmniej 30 minutach.
7. Wszystkie systemy uwierzytelniania muszą kontrolować okres nieaktywności/nieużywania loginu, który nie powinien przekraczać 100 dni. Jeśli jest to technicznie możliwe, użytkownik lub inna upoważniona osoba mogą ponownie aktywować dezaktywowane loginy.
8. Proces uwierzytelniania musi potwierdzić, że tego samego hasła nie używano w ciągu co najmniej sześciu (6) ostatnich zmian hasła.

17.21 Korzystanie z narzędzi systemowych

Dostawca musi zadbać o to, aby korzystanie z programów narzędzi, które mogą obejść środki kontroli systemu i aplikacji (np. uruchamianie z urządzeń zewnętrznych), było ograniczone i kontrolowane.

17.22 Przekroczenie limitu czasu sesji

1. W przypadku wszystkich użytkowników Kontrolowanych Systemów Informatycznych wykorzystywanych do przechowywania, przetwarzania i/lub przesyłania Informacji Citi należy przeprowadzić ponowne logowanie lub uwierzytelnienie.
2. Konieczne jest wymaganie od Użytkowników ponownego uwierzytelnienia po okresie nieaktywności, który nie przekracza 30 minut. Aktywność obejmuje wszelkie dane wprowadzane na punkcie końcowym (mysz, klawiatura, ekran dotykowy itp.). Jeśli zastosowano wygaszacz ekranu chroniony hasłem, zastosowanie aplikacji/jednorazowej rejestracji nie jest konieczne.

17.23 Zakończenie dostępu użytkownika

1. Po rozwiązaniu umowy o pracę lub rezygnację z pracy należy niezwłocznie usunąć dostęp i odebrać użytkownikowi uprawnienia, które mogłyby umożliwić dostęp do Informacji Citi sklasyfikowanych jako Poufne lub

o wyższej klauzuli tajności (m.in. logowanie się użytkownika do pulpitu, usługi Active Directory, Single Sign-On (SSO), poczta elektroniczna, tokeny One Time Password (OTP) i dostęp zdalny).

2. Jeśli pracownik ma dostęp do systemów będących własnością Citi i administrowanych przez Citi, Menedżer ds. relacji biznesowych w Citi, Właściciel Działów Biznesowych lub zastępca Właściciela Działów Biznesowych muszą zostać niezwłocznie poinformowani o zmianie stanowiska pracownika lub o rozwiązaniu umowy o pracę z tym pracownikiem, tak by zapewnić, że Menedżer ds. relacji biznesowych w Citi zainicjuje usunięcie dostępu zwolnionego pracownika przed datą końca obowiązywania umowy o pracę.
3. Dostawca ma wdrożony udokumentowany proces odzyskiwania dostępu ze wszystkich aktywów zgodnie z ramami czasowymi określonymi w punkcie 17.23.2 na wypadek rozwiązania umowy o pracę lub rezygnacji pracownika albo osoby niebędącej pracownikiem.
4. Jeśli Dostawca odkryje jakąkolwiek nieprawidłowość w odniesieniu do punktów 17.23.1–17.23.3, musi niezwłocznie powiadomić o tym fakcie Menedżera ds. relacji biznesowych w Citi, Właściciela Działów Biznesowych lub zastępcę Właściciela Działów Biznesowych, podając uzasadnienie i przewidziane środki kontroli.

17.24 Dostęp zdalny

Dostawca musi wdrożyć mechanizmy kontroli zdalnego dostępu w celu ochrony dostępu do sieci, w których mogą być przechowywane, przetwarzane lub przekazywane dane Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności, co obejmuje:

1. Zdalny dostęp do Systemów informatycznych wykorzystywanych do przechowywania, przetwarzania, przesyłania Informacji Citi oraz zarządzania nimi należy chronić przed nieupoważnionym wykorzystaniem.
2. Wszystkie zarządzane przez Dostawcę laptopy i zarządzane przez Dostawcę komputery stacjonarne wykorzystywane do przechowywania, przetwarzania i/lub przesyłania Informacji Citi, wykorzystujące zdalny dostęp w sytuacji, gdy lokalnie przechowywane/przetwarzane są Informacje Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności, należy zaszyfrować z wykorzystaniem narzędzia szyfrującego, które spełnia standardy branżowe.
3. Dostęp zdalny może odbywać się wyłącznie za pośrednictwem zatwierdzonych rozwiązań zdalnego dostępu, które wykorzystują uwierzytelnianie wieloskładnikowe (MFA).
4. Jeśli urządzenia obsługiwane przez Dostawcę są połączone z Internetem bezpośrednio (tj. nie poprzez zaporę lub serwer proxy Dostawcy), muszą mieć włączoną zaporę sieciową.
5. Urządzenia zarządzane przez Dostawcę muszą być regularnie podłączane do sieci Dostawcy, aby umożliwić regularne otrzymywanie i instalowanie aktualizacji oprogramowania i narzędzi antywirusowych, co stanowi wymóg zapewniający pełny dostęp do sieci. Ograniczony dostęp może być dozwolony do ściśle określonego celu aktualizacji urządzenia.
6. Jeśli w celu uzyskania dostępu do danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności używane są urządzenia, które nie są własnością Dostawcy i nie są przez niego zarządzane, takie urządzenia muszą być skonfigurowane do korzystania z autoryzowanego rozwiązania,

które nie pozwala na pobieranie danych na lokalny komputer. Należy wdrożyć następujące mechanizmy kontroli:

- a) Zabronione jest pobieranie danych Citi na urządzenia, które nie są zarządzane przez firmowe rozwiązania programowe.
 - b) Dostawca musi zadbać o to, aby taki dostęp był chroniony poprzez uwierzytelnienie oparte na tokenie lub certyfikacie, wykorzystujące standardowe technologie zdalnego dostępu (np. Virtual Desktop Interface (VDI)).
 - c) Rozwiązania umożliwiające zdalny dostęp, takie jak Terminal Services i VMware Horizon, muszą zostać skonfigurowane tak, aby wyłączyć udostępnianie zawartości schowka i mapowanie dysków przez protokoły Blast, PCoIP, RDP i SSH.
7. Jeśli na potrzeby MFA używane są tokeny oprogramowania, np. w celu uzyskania dostępu do aplikacji na urządzeniu mobilnym, oprogramowanie do uwierzytelniania tokenów oprogramowania musi uwierzytelniać użytkownika (np. za pomocą hasła, danych biometrycznych itp.) i zapobiegać użyciu tego oprogramowania, jeśli dojdzie do „jailbreaku” telefonu komórkowego lub jego zrootowania (przy użyciu systemu operacyjnego innego niż certyfikowany i dostarczony przez dostawcę urządzenia mobilnego).
8. Cały Personel Dostawcy, w tym m.in. pracownicy stali/tymczasowi, kontrahenci i podwykonawcy, wymagający specjalnego, uprzywilejowanego i/lub administracyjnego dostępu do systemów, repozytoriów danych, aplikacji i/lub infrastruktury, w tym m.in. administratorzy systemów, administratorzy baz danych, administratorzy kontroli dostępu, administratorzy zapory sieciowej, administratorzy witryn internetowych itp., którzy są bezpośrednio lub pośrednio związani z Usługami świadczonymi na rzecz Citi, muszą korzystać wyłącznie z uwierzytelniania wieloskładnikowego (MFA), a dostęp ten będzie niezależnie rejestrowany i monitorowany przez Dostawcę pod kątem podejrzanej aktywności i/lub nieautoryzowanego dostępu zgodnie z niniejszymi Wymaganiami.
9. W przypadku urządzeń osobistych i urządzeń należących do strony trzeciej Dostawca musi dysponować skutecznym rozwiązaniem gwarantującym, że takie urządzenia mają zatwierdzoną wersję systemu operacyjnego, odpowiednie poziomy poprawek, rozwiązania antywirusowe i chroniące przed złośliwym oprogramowaniem, zanim takie urządzenia będą mogły zalogować się do sieci.
10. Dostawca musi dopilnować następujących wymogów:
- a) Utrzymywanie prywatnej, wydzielonej zdalnej przestrzeni roboczej, w której nie ma żadnych urządzeń obsługujących asystentów głosowych (np. Siri, Alexa), urządzeń do nagrywania wideo i/lub innych urządzeń do odsłuchu/nagrywania zdjęć, wideo lub audio. Nieupoważniony personel nie będzie mógł przeglądać żadnych danych, systemów, aplikacji, które mogą pojawić się na ekranie (ekranach) zdalnych systemów komputerowych.

- b) Zablokowanie komputera w przypadku pozostawienia go bez nadzoru, aby w odpowiedni sposób ograniczyć nieautoryzowany dostęp do ekranu.

17.25 Zasada czystego biurka

Personel Dostawcy ma obowiązek chronić Informacje Citi w każdej formie, w tym informacje w formie fizycznej wykorzystywane lub przechowywane w przestrzeni roboczej takiego personelu. Dostawcy są zobowiązani do informowania o tym wymogu wszystkich swoich pracowników co najmniej raz w roku poprzez szkolenie w zakresie bezpieczeństwa informacji lub za pośrednictwem innego kanału komunikacji.

17.26 Bezpieczeństwo przeciwpożarowe

1. Dostawca musi przestrzegać obowiązujących wymogów prawnych i regulacyjnych w zakresie bezpieczeństwa fizycznego oraz stworzenia bezpiecznego środowiska pracy, w tym lokalnych przepisów przeciwpożarowych.
2. Dostawca musi stosować systemy wykrywania pożaru, alarmowania o pożarze i zwalczania go. Takie systemy należy poddawać kontroli co pół roku i testować raz w roku.

17.27 Bezpieczeństwo fizyczne

1. Informacje Citi muszą być przechowywane w bezpiecznych miejscach, do których dostęp ma wyłącznie upoważniony do tego personel.
2. Dostawca musi wdrożyć udokumentowany system fizycznego dostępu, który będzie można poddać kontroli.
3. Dostawca musi korzystać z połączenia systemów alarmowych/antywłamaniowych, które obejmują alarm bezpieczeństwa monitorowany przez stronę trzecią, strażników i nadzór wideo, odpowiednio do środowiska i świadczonych usług.
4. Dostawca musi mieć udokumentowaną politykę dotyczącą gości, która będzie wymagać od wszystkich gości okazania weryfikowalnego dokumentu tożsamości po przybyciu, wpisaniu się i wypisaniu.

17.28 Procedury bezpieczeństwa operacyjnego i odpowiedzialność

1. Proces zarządzania zmianą po stronie Dostawcy musi obejmować kluczowe punkty kontrolne związane z rejestracją zmiany, przeglądem, testowaniem, zatwierdzaniem, wdrażaniem i finalizowaniem. Dostawca musi również wdrożyć awaryjny proces zmian, który musi obejmować wszystkie określone etapy oraz wymagać przestrzegania hierarchii zatwierdzeń.
2. Dostawca musi mieć wdrożony podlegający audytowi proces zarządzania wydajnością, który obejmuje (ale nie ogranicza się do) wskaźniki dostępności, przepustowości i wydajności; ocenę wpływu na działalność; proaktywne śledzenie, badanie i rozwiązywanie problemów związanych z wydajnością i przepustowością.
3. W stosownych przypadkach Dostawca musi zadbać o pełne fizyczne lub logiczne rozdzielenie środowisk laboratorium, programowania, testowania i produkcji.

17.29 Wymogi dotyczące tworzenia oprogramowania

Mają zastosowanie do Dostawców dostarczających oprogramowanie opracowane wyłącznie do użytku Citi. Dostawcy muszą przestrzegać tych wymogów lub wykazać udokumentowany i zatwierdzony proces cyklu życia oprogramowania („SDLC”, Software Development Lifecycle) o równoważnym podejściu zapewniającym równorzędną jakość.

17.30 Inicjowanie i planowanie

Dostawca musi określić zakres i cele rozwiązania zgodnie z wymogami Citi i zobowiązaniami umownymi. Obejmuje to:

1. Dokumentowanie wymagań funkcjonalnych i pozafunkcjonalnych;
2. Dostarczanie szacunków dotyczących nakładu pracy i terminów realizacji; oraz
3. Identyfikowanie wszystkich komponentów lub zależności pochodzących od stron trzecich.

Działania w zakresie zgodności, w tym oceny ryzyka związanego z bezpieczeństwem, należy rozpocząć już na samym początku projektu. Role, obowiązki i punkty kontrolne zatwierdzenia należy zakomunikować w sposób jasny.

Wszystkie środowiska muszą być sklasyfikowane jako Rozwój (DEV), Testowanie (TEST) lub Produkcja (PROD) i pozostać ściśle odseparowane przez cały cykl życia. Klasyfikacja środowiska określa uprawnienia dostępu i rodzaj danych, które mogą być przetwarzane. Dostawca musi ograniczyć dostęp na podstawie przypisanej klasyfikacji środowiska i dostosować wdrożenia do odpowiedniej fazy SDLC, aby zapobiec nieautoryzowanemu dostępowi lub ujawnieniu danych.

17.31 Projekt

Dostawca musi udokumentować podejście projektowe, które zapewnia, że dostarczone rozwiązanie spełnia wszystkie określone wymagania („Plan testów”). Jako wymóg minimalny, Plan testów musi zawierać i opisywać:

1. Wszystkie testy, które mają zostać przeprowadzone przez zespół ds. rozwoju, w tym testy jednostkowe oraz testy funkcjonalne i pozafunkcjonalne, a także testy dotyczące aspektów wydajności, z możliwością odniesienia do wymagań;
2. Identyfikację osób zatwierdzających, które potwierdzą ukończenie;
3. Wymagania dotyczące testów bezpieczeństwa, takie jak oceny luk w zabezpieczeniach i modelowanie zagrożeń; oraz
4. Środowisko testowe, podejście, proces i ścieżkę wdrażania.

Należy przygotować strategię udostępniania, określającą warunki wstępne i proces wdrażania do środowisk TEST i PROD, w tym kryteria gotowości do wydania, zawartość i harmonogram dostarczania w okresie trwania projektu.

Jeśli określono to w Umowie, dystrybucja oprogramowania musi być pakietowana w formacie zatwierdzonym przez Citi, korzystając z zatwierdzonych przez Citi narzędzi oraz przepływów pracy.

17.32 Testowanie

Testy muszą być planowane i przeprowadzane w środowisku kontrolowanym w celu potwierdzenia, że rozwiązanie spełnia określone wymagania i kryteria skuteczności.

Przypadki testowe muszą zapewniać możliwość odniesienia do wymagań i zatwierdzeń kodu.

Dostawca powinien przygotować raport podsumowujący wyniki testów pozytywnych/negatywnych, dodatkowe testy przeprowadzone w trakcie fazy rozwoju oraz wszelkie testy, które nie zostały ukończone (wraz z uzasadnieniem) („Raport końcowy z testu”). Wady i odroczone funkcje muszą być udokumentowane wraz z planami działań zaradczych dotyczących nierozwiązanych problemów.

Na żądanie Citi Dostawca musi przedstawić dowody:

1. Przygotowania szczegółowego planu testów;
2. Ukończenia testu i wyniki szczegółowo opisane w Raporcie końcowym z testu; oraz
3. Odniesienie wyników testów do wymagań i zatwierdzeń kodu.

17.33 Wdrażanie

Przed wdrożeniem Dostawca musi przeprowadzić wszystkie wymagane testy bezpieczeństwa, w tym skanowanie luk w zabezpieczeniach i modelowanie zagrożeń. Proces wdrażania musi być uporządkowany i dokumentować rejestry zmian, strategie wycofywania i wymagane zatwierdzenia. Plany wdrażania i instrukcje wdrażania (runbooki) muszą zawierać protokoły monitorowania i eskalacji.

Po wdrożeniu Dostawca musi sfinalizować identyfikatory systemu i zaktualizować wszystkie powiązane artefakty, aby zapewnić gotowość do audytu.

17.34 Bezpieczeństwo

1. Ustrukturyzowana ocena przeprowadzana w fazie projektowania SDLC w celu zidentyfikowania i rozwiązania potencjalnych zagrożeń bezpieczeństwa, luk w zabezpieczeniach i niedoskonałości architektury systemu przed napisaniem kodu („Przegląd projektu zabezpieczeń”) musi zostać uwzględniona w procesie SDLC wraz ze środkami zapobiegawczymi i wykrywającymi zgodnymi ze standardami branżowymi, takimi jak OWASP.
2. Należy egzekwować bezpieczne praktyki kodowania.
3. Dostawca musi wdrożyć środki kontroli w zakresie bezpieczeństwa informacji do swoich procesów i procedur dotyczących wyboru, rozwoju i wdrażania aplikacji, produktów i usług.
4. Dostawca musi zapewnić procedurę bezpiecznej kompilacji dla wszystkich systemów, w których przechowywane, przetwarzane i/lub przesyłane są Informacje Citi, oraz musi utrzymywać bezpieczny obraz lub szablon dla wszystkich systemów.

17.35 Środki kontroli w celu ochrony przed złośliwym oprogramowaniem

Dostawca musi zadbać o wdrożenie środków kontroli w celu wykrywania przypadków umieszczania w oprogramowaniu złośliwego kodu (np. wirusów, robaków, koni trojańskich, oprogramowania z reklamami, oprogramowania szpiegującego, oprogramowania ransomware lub innych podobnych cyberataków, w których może dojść do naruszenia danych) i zapobiegania takim przypadkom. Dostawca musi:

1. Instalować, aktualizować i utrzymywać technologię przeciwdziałającą wirusom i oprogramowaniu szpiegującemu na wszystkich komputerach osobistych, jak również technologię na wszystkich serwerach sieci lokalnej

- (LAN), serwerach poczty elektronicznej i innych urządzeniach przechowujących, przetwarzających i/lub transmitujących dane Citi.
2. Zapewnić wdrożenie ustawień bezpieczeństwa, które uniemożliwiają użytkownikom końcowym wyłączenie narzędzi antywirusowych/anty-malware i zaplanowanych operacji skanowania.
 3. Zapewnić centralny i zautomatyzowany system zarządzania procedurami konfiguracji oraz aktualizacji oprogramowania antywirusowego i anty-malware.
 4. Zapewnić wdrożenie procesów identyfikacji i aktualizowania komputerów niezgodnych z wymogami, w których sygnatury antywirusowe lub silniki skanujące są przestarzałe.
 5. Kontrolować dostęp do portów/interfejsów komunikacyjnych, które umożliwiają łączenie z urządzeniami zewnętrznymi, między innymi z nośnikami pamięci masowej.

17.36 Środki kontroli przeciwko kodowi mobilnemu

Dostawcy muszą zapewnić wdrożenie środków kontroli w zakresie bezpiecznych praktyk dotyczących kodu mobilnego. Gdy kod mobilny zostanie autoryzowany, konfiguracja, jako minimum, musi spełniać wszystkie odnośne standardy branżowe i zobowiązania umowne wobec Citi, a Dostawca zapewniać, że autoryzowany kod mobilny działa zgodnie z jasno zdefiniowaną i udokumentowaną polityką bezpieczeństwa oraz zapobiegać działaniu nieautoryzowanego kodu mobilnego.

W przypadku kodu mobilnego, który może mieć wpływ na system operacyjny lub platformę (tj. poza „piaskownicą”), Dostawca musi zadbać o następujące kwestie:

1. Kod mobilny opublikowany przez Dostawcę musi być podpisany przez zatwierdzony przez Citi Organ Certyfikujący; Dostawca musi pilnować okresu ważności takiego certyfikatu, by odpowiednio zareagować w przypadku jego wygaśnięcia lub odnowienia.
2. Podpisany kod mobilny z wygasłymi certyfikatami musi zostać usunięty z produkcji.

17.37 Rejestrowanie wyników audytu

Dostawca musi dopilnować, by wszystkie Kontrolowane Systemy Informatyczne wykorzystywane do uzyskiwania dostępu do danych Citi, przechowywania, przetwarzania, przesyłania Informacji Citi i/lub zarządzania nimi stosowały ścieżkę audytu na poziomie infrastruktury lub aplikacji, by rejestrować następujące elementy:

1. Działania związane z bezpieczeństwem infrastruktury dla powiązanej platformy
2. Wszystkie alarmy systemowe powiązane z zaporą lub zdarzeniem związanym z bezpieczeństwem wygenerowanym przez System Wykrywania Włamań / System Zapobiegania Włamaniom
3. Wszystkie próby naruszenia bezpieczeństwa systemu (np. nieudane próby logowania się Użytkownika)
4. Nieautoryzowane próby dostępu do zasobów (oprogramowania, danych, procesów itp.)

5. Działania administratora
6. Informacje związane z otrzymaniem określonych informacji od użytkownika lub innego systemu
7. Wszystkie istotne zdarzenia związane z transakcjami finansowymi oraz Informacjami Citi zawierającymi zwłaszcza następujące elementy:
 - a. Aktualizacje transakcji finansowych;
 - b. Aktualizacje Poufnych Informacji Umożliwiających Ustalenie Tożsamości lub Wrażliwych Informacji Umożliwiających Ustalenie Tożsamości
 - c. Aktualizacje Danych Zastrzeżonych;
 - d. Aktualizacje Danych uwierzytelniających.
8. Wszystkie nawiązane sesje
9. Jeśli jest to technicznie możliwe, należy zapisywać artefakty sesji, takie jak unikatowy identyfikator urządzenia, a także rejestrować je dla aplikacji mających dostęp do danych Citi (np. witryn internetowych i aplikacji mobilnych), by pomóc w przeprowadzaniu postępowań wyjaśniających w sprawie oszustw. Te artefakty muszą zawierać co najmniej adresy IP. Należy zapisywać takie artefakty w przypadku transakcji Citi oraz otwierania rachunku w Citi. Informacje należy zapisywać tak, aby możliwe było powiązanie artefaktu sesji z transakcją lub otwarciem rachunku.
10. Ścieżki audytu muszą dokumentować przypisanie określonej działalności konkretnej osobie, aby zapobiec wyparciu się takiego działania.
11. Należy rejestrować istotne zdarzenia w zakresie Administrowania Bezpieczeństwem Informacji (ISA), zwłaszcza takie, które obejmują:
 - a) utworzenie użytkownika;
 - b) modyfikację praw dostępu użytkownika;
 - c) usunięcie, utworzenie i zmiana profili w Kontrolowanym Systemie Informatycznym;
 - d) resetowanie hasła;
 - e) zmiany w konfiguracji bezpieczeństwa systemu;
 - f) wszystkie interaktywne działania uprzywilejowanych Identyfikatorów funkcjonalnych;
 - g) rejestry bezpieczeństwa muszą zawierać co najmniej następujące informacje, niezależnie od systemu generującego rejestr, chyba że takie włączenie nie jest technicznie możliwe:
 - I. data i godzina zdarzenia (format czasu: UTC);
 - II. identyfikator Użytkownika wykonującego dane działanie;
 - III. rodzaj zdarzenia;
 - IV. Nazwa zasobu lub aktywa;
 - V. Rodzaj dostępu (usuwanie, zmiana itp.);
 - VI. Powodzenie lub niepowodzenie zdarzenia;
 - VII. źródło (terminal, port, lokalizacja, IP, nazwa hosta itp.).

17.38 Ochrona danych w rejestrach

Dostawca musi zapewnić wdrożenie środków kontroli w celu zachowania integralności ścieżek audytu na etapie uruchamiania, wyłączania, przechowywania i przesyłania.

1. Aby zapobiec nieupoważnionym zmianom rejestrów audytowych, Dostawca musi zadbać o to, aby takich rejestrów nie mogli nadpisać ani zmienić użytkownicy systemu, których aktywność jest w nich zapisywana.
2. Dostawca musi przedstawić Citi procedurę przechowywania danych rejestrowych, która określa, jak przechowywane są dane, i obejmuje środki zgodności uwzględniające wszystkie obowiązujące wymogi prawne i regulacyjne.
3. Zegary wszystkich istotnych systemów przetwarzających informacje w organizacji lub domenie bezpieczeństwa należy synchronizować według dokładnego źródła czasu.

17.39 Korzystanie z systemu monitorowania

Dostawcy muszą zadbać o zapisywanie, rejestrowanie i weryfikowanie następujących zdarzeń bezpośrednio lub poprzez zautomatyzowany proces weryfikacji:

1. Wszystkie alarmy systemowe powiązane z zaporą lub Systemami Wykrywania Włamań (IDS) / Systemem Zapobiegania Włamaniom (IPS), które wygenerowały zdarzenie związane z bezpieczeństwem.
2. Wszystkie aktualizacje zasobów o krytycznym znaczeniu, określonych w bezpiecznej standardowej kompilacji.
3. Wszelkie interaktywne działania wykonywane przy użyciu dowolnych identyfikatorów (funkcjonalnych, uprzywilejowanych, systemowych, tymczasowych itp.) z dostępem do informacji sklasyfikowanych jako Poufne umożliwiające ustalenie tożsamości lub o wyższej klauzuli tajności.
4. Istotne zdarzenia w zakresie Administrowania Bezpieczeństwem Informacji, wymienione w powyższej sekcji Rejestrowanie wyników audytu, z następującym wyjątkiem:
 - a) Usuwanie uprawnień, roli lub profilu użytkownika w sytuacjach, w których używany jest zautomatyzowany przepływ pracy / system realizacji wykorzystujący kompleksowe środki kontroli przeprowadza działanie z zakresu Administrowania Bezpieczeństwem Informacji.

17.40 Korelacja i przegląd dzienników zdarzeń

1. Jeśli zarejestrowane zostanie zdarzenie wyzwalające alarm, a zdarzenie jest przeglądane, Dostawca musi zainicjować działania następcze i rozpocząć dochodzenie, zwłaszcza jeżeli zdarzenie wskazuje na potencjalny incydent naruszenia bezpieczeństwa informacji.
2. Dostawca musi dopilnować, aby rejestry audytowe były agregowane w centralnym systemie zarządzania dziennikami, takim jak system SIEM (Security Information and Event Management) lub narzędzie do analizy dzienników w celu analizy korelacji i przeglądu dzienników.
3. Dostawcy mają obowiązek dokonywania okresowych przeglądów i zmian konfiguracji swojego systemu SIEM lub narzędzia do analizy dzienników zdarzeń, aby usprawnić identyfikację określonych zdarzeń, względem których należy podjąć działania.

17.41 Kontrola nad oprogramowaniem użytkowym

Dostawca musi zapewnić, że zastosuje wyłącznie takie systemy operacyjne i oprogramowanie, które w chwili obecnej wspiera renomowany w branży podmiot komercyjny, lub takie, do których dostępne są aktywne i odpowiednie poprawki oraz uaktualnienia konfiguracyjne mające na celu poprawę bezpieczeństwa.

Dostawca musi zapewnić, że wdroży udokumentowany proces, który ustanawia ramy czasowe zastosowania wszystkich poprawek dotyczących bezpieczeństwa.

Niezależnie od jakichkolwiek innych umów dotyczących obsługi zawartych między Dostawcą a Citi, Dostawca musi zapewnić, że oprogramowanie wydane dla Citi i obłożone umową licencji nie dopuszcza korzystania z wersji oprogramowania nieobjętego wsparciem, które ma znane luki w zabezpieczeniach oraz jest aktualizowane i łatanie zgodnie z wymaganiami w odpowiednim czasie.

Oprogramowanie wykorzystywane do przetwarzania Informacji Citi musi być nabywane od sprawdzonych Dostawców wraz z pakietem licencji, katalogu i wsparcia.

17.42 Zarządzanie lukami w zabezpieczeniach i zagrożeniach

1. Dostawca musi wdrożyć proces zarządzania lukami w zabezpieczeniach i zagrożeniami, który kompleksowo uwzględnia i/lub obejmuje wszystkie poniższe elementy:
 - a. Narzędzia i procedury do wykrywania słabych punktów i zarządzania nimi we wszystkich aktywach, które mogą być wykorzystywane do przetwarzania, przechowywania, uzyskiwania dostępu lub przekazywania poufnych lub wyższej klauzuli wrażliwości danych Citi.
 - b. Wymóg przeprowadzania skanów co najmniej raz w tygodniu za pomocą uznanego w branży narzędzia do zarządzania lukami w zabezpieczeniach i zgodnie z metodologią zgłaszania.
 - c. Ranking podatności na zagrożenia zgodnie z najbardziej aktualną wersją systemu oceny „Common Vulnerability Scoring System (CVSS)” (patrz <https://www.first.org/cvss>), wraz z harmonogramem działań naprawczych w zależności od stopnia ich istotności.
 - d. Wymóg testowania poprawek luk w zabezpieczeniach przed pełnym wdrożeniem do procesu produkcji.
 - e. Udokumentowany i powtarzalny proces roboczy przyspieszania działań naprawczych związanych z krytycznymi lukami w zabezpieczeniach.
 - f. Dostawca musi monitorować aktywa przez cały cykl ich obsługi, aby przygotować się na statusy zakończenia okresu eksploatacji (EOL, End of Life) lub wsparcia technicznego (EOVS, End of Vendor Support). Musi on również wdrożyć procesy mające na celu aktualizację/modernizację lub wymianę takich aktywów.
 - g. Wszelkie luki w zabezpieczeniach określone w systemie CVSS jako krytyczne, zidentyfikowane poprzez gromadzenie informacji, skanowanie luk w zabezpieczeniach lub testy penetracyjne muszą mieć przypisany najwyższy priorytet i być usuwane w odpowiednio zdefiniowanych ramach czasowych współmiernych do odnośnego ryzyka.

17.43 Aplikacje hostowane przez Strony trzecie

Jeżeli Dostawca utrzymuje lub przechowuje w witrynie internetowej, systemie dostępnym przez Internet albo w witrynie internetowej pod marką Citi dane Citi sklasyfikowane jako Poufne lub o wyższym poziomie wrażliwości, wówczas w celu ochrony przed podatnością na zagrożenia lub zagrożeniem, które dotyczy produktów lub usług mających wpływ na Citi (każda z nich zwana dalej „Luką w zabezpieczeniach”), Dostawca musi przestrzegać następujących wymagań:

1. Wyznaczyć jednego pracownika Dostawcy do odpowiadania na zapytania Citi dotyczące bezpieczeństwa informatycznego.
2. Korzystać z renomowanych w branży praktyk w celu monitorowania wiarygodnych źródeł informacji o lukach w zabezpieczeniach komputerów, takich jak FIRST, CERT/CC, katalog znanych luk w zabezpieczeniach CISA Known Exploited Vulnerabilities Catalog i listy mailingowe dostawców, a także podejmować odpowiednie środki w celu uzyskania, dokładnego przetestowania, zastosowania i dostarczenia Citi odpowiednich dodatków Service Pack, poprawek, aktualizacji i obejść.
3. Co najmniej raz na kwartał testować wdrożenie środków bezpieczeństwa informacji za pomocą narzędzi do skanowania luk w zabezpieczeniach sieci, systemu oraz aplikacji i/lub testów penetracyjnych.
4. Zezwolić Citi lub stronie trzeciej zatwierdzonej przez Citi na przeprowadzenie, w rozsądnych odstępach czasu, oceny luk w zabezpieczeniach, etycznych hacków lub innych ocen bezpieczeństwa w celu weryfikacji przestrzegania przez Dostawcę jego zobowiązań wynikających z dowolnej umowy i niniejszych Wymagań, w tym m.in. przeglądu polityk, procesów i procedur, oceny na miejscu rozwiązań dotyczących bezpieczeństwa fizycznego, skanowania sieci, systemu i aplikacji pod kątem luk w zabezpieczeniach oraz testów penetracyjnych przy użyciu dostępnych na rynku narzędzi i/lub standardowych praktyk branżowych w celu przeprowadzenia tych kontroli.
5. Każdy podwykonawca, który zapewnia Dostawcy usługi oceny podatności na zagrożenia, musi znajdować się na zatwierdzonej przez Citi liście dostawców usług oceny podatności na zagrożenia. Jeśli Dostawca świadczy Usługi poprzez wykonawców lub podwykonawców, Dostawca na własny koszt musi dopilnować, aby wszelkie oceny luk w zabezpieczeniach wymagane na mocy niniejszych wymagań zostały przeprowadzone w takim samym terminie, jak gdyby Dostawca świadczył te Usługi bezpośrednio. Dostawca musi także zapewnić, że wymóg przeprowadzenia takich ocen stawiany każdemu wykonawcy lub podwykonawcy zostanie zapisany w umowie między Dostawcą a wykonawcą/podwykonawcą odnośnie do danej Usługi, co będzie obejmować upoważnienie Citi do przeprowadzania takich ocen.
6. **Powiadomienie.**
 - a) W przypadku stwierdzenia przez Dostawcę luki w zabezpieczeniach, która dotyczy produktu lub usługi Citi, Dostawca musi powiadomić Citi na piśmie w ciągu 24 godzin od wykrycia Luki i uwzględni opis działań naprawczych podejmowanych przez Dostawcę.

b) W przypadku stwierdzenia przez Dostawcę luki w zabezpieczeniach, która dotyczy produktu lub usługi wpływającej na Citi, w następstwie odpowiedzialnego publicznego ujawnienia kanałów procesu (publikacja Podatności na zagrożenia w National Vulnerability Database (NVD) lub za pośrednictwem katalogu zagrożeń udostępnianego zewnętrznym dostawcom zabezpieczeń), Dostawca powiadomi Citi na piśmie w ciągu 24 godzin od takiej publikacji. Każde powiadomienie musi zawierać informację o luce w zabezpieczeniach, przydatności systemu w kontekście usług Citi (tj. czy przechowuje on informacje Citi lub jest wykorzystywany do świadczenia usług lub jedno i drugie), informację, czy można taką lukę wykorzystać zdalnie, a także wynik CVE (Common Vulnerabilities and Exposures). Dostawca będzie kontynuować dostarczanie Citi aktualizacji do czasu usunięcia luki w zabezpieczeniach. Jeśli Citi zidentyfikuje lukę w zabezpieczeniach, może powiadomić o tym fakcie Dostawcę, a Dostawca niezwłocznie usunie taką lukę zgodnie z niniejszą Częścią.

7. **Środki zaradcze.** W przypadku każdej Luki w zabezpieczeniach strona zgłaszająca oceni poziom ryzyka i wpływ takiej luki w oparciu o wagę i ryzyko dla Citi oraz przypisze priorytet ryzyka na podstawie systemu Common Vulnerability Scoring System (CVSS) zgodnie z Załącznikiem A do niniejszego dokumentu (patrz <https://www.first.org/cvss>). Po przypisaniu i uzgodnieniu poziomu ryzyka przez strony Dostawca naprawi wszelkie luki w zabezpieczeniach o poziomie określonym jako średni, wysoki lub krytyczny. O ile to możliwe, poprawki wszelkich takich luk w zabezpieczeniach powinny zostać udostępnione w pakiecie zabezpieczeń dla aktualnie wdrożonego wydania.

Jeśli Dostawca nie jest w stanie lub nie chce usunąć Luki w zabezpieczeniach w sposób satysfakcjonujący Citi, Citi może wypowiedzieć stosowną licencję bez jakiegokolwiek dalszej odpowiedzialności lub zobowiązań finansowych (w odniesieniu do części rozwiązanej), a Dostawca niezwłocznie zwróci Citi proporcjonalną część zapłaconych opłat licencyjnych.

17.44 Środki kontroli sieci bezpieczeństwa komunikacji

1. Sieci Dostawcy wykorzystywane do uzyskiwania dostępu do Informacji Citi, a także ich przechowywania, zarządzania nimi, ich przetwarzania i/lub przesyłania należy chronić przed zagrożeniami; konieczne jest zadbanie o bezpieczeństwo Systemów Informatycznych za pomocą sieciowych punktów egzekwowania.

- a. Informacje sklasyfikowane przez Citi jako Poufne lub o wyższej klauzuli tajności nie mogą być trwale przechowywane w systemie w strefie zdemilitaryzowanej (DMZ) z dostępem do Internetu. Sieci używane do uzyskiwania dostępu do Informacji Citi, ich przechowywania, zarządzania nimi, ich przetwarzania i / lub przesyłania za pomocą bezprzewodowych sieci lokalnych (WLAN) lub innych rozwiązań urządzeń bezprzewodowych, które obejmują uzasadnione mechanizmy kontroli uniemożliwiające nieautoryzowany dostęp (PEAP-TLS, EAP-TTLS itp.), mogą być połączone z sieciami zawierającymi Informacje Citi.
 - b. Wszystkie zewnętrzne połączenia IP z globalną siecią Dostawcy muszą być chronione przez zaporę, którą zarządza Dostawca.
 - c. Wdrożono działający w czasie rzeczywistym System Wykrywania Włamań (IDS, Intrusion Detection System) i System Zapobiegania Włamaniom (IPS, Intrusion Prevention System), który monitoruje i chroni połączenia internetowe z siecią Dostawcy, w której uzyskiwany jest dostęp do Informacji Citi, a także Informacje te są przechowywane, zarządzane, przetwarzane lub przesyłane.
2. W przypadku wszystkich aplikacji internetowych oznaczonych marką Citi Dostawca musi spełnić następujące wymogi:
- a. Usługi znajdujące się w witrynach internetowych Dostawcy są chronione przez usługi zapobiegające atakom DDoS (rozproszonej odmowie usługi) lub porównywalne środki kontroli zatwierdzone przez Citi.
 - b. W przypadku zewnętrznych zapór musi być stosowana domyślna reguła „odrzuć wszystko”. Reguły zapory sieciowej muszą być skonfigurowane w oparciu o zasadę przydzielania najmniejszych uprawnień, a wszystkie próby połączeń, które są blokowane przez zaporę (np. odrzucanie pakietów), powinny być rejestrowane.
 - c. Odmowa ruchu komunikacji sieciowej musi być ustawieniem domyślnym, a na zarządzanych interfejsach zezwolenie jest włączone wyjątkowo. Wyjątki muszą być bardzo ograniczone do konkretnych źródeł, miejsc docelowych i usług.
 - d. Ruch w aplikacji webowej powinien podlegać odpowiednim kontrolom i być filtrowany, na przykład przez zapory aplikacji sieciowych (Web Application Firewall).

17.45 Segregacja w sieciach

Dostawca musi dopilnować, aby wszystkie Systemy informatyczne i aplikacje, które są wykorzystywane do uzyskiwania dostępu do danych Citi, przechowywania, przetwarzania, przesyłania Informacji Citi i/lub zarządzania nimi oraz do których można uzyskać dostęp przez Internet, były dostępne wyłącznie poprzez strefę zdemilitaryzowaną (DMZ) Dostawcy.

Podczas zdarzenia kryzysowego Dostawca musi być w stanie filtrować dostęp między częściami sieci, aby zmniejszyć wpływ Zdarzeń związanych z bezpieczeństwem sieci (np. filtrowanie portów podczas wybuchu wirusa).

Dostęp zdalny i Zabezpieczenia hostów muszą uwzględniać środki kontroli dostępu oparte na grupach (np. dostęp dla personelu, podwykonawców), aby ograniczyć dostęp do zasobów sieciowych w sieci Dostawcy. Na poziomie hosta kontrolę dostępu można sprawować z poziomu grupy lub poziomu indywidualnego.

17.46 Identyfikacja urządzeń w sieciach

Platformy technologiczne muszą identyfikować i uwierzytelniać równorzędne platformy technologiczne współmiennie do poziomów zagrożenia bezpieczeństwa informacji dla interakcji i z uwzględnieniem innych mechanizmów kontrolnych ograniczających ryzyko.

1. Do Sieci Dostawcy, w której Informacje Citi są przechowywane, przetwarzane lub przesyłane, mogą mieć dostęp wyłącznie urządzenia Dostawcy (tj. sprzęt komputerowy, w tym w szczególności: komputery osobiste i laptopy) zgodne z niniejszymi wymogami i autoryzowane przez Dostawcę.
2. Do sieci Citi mogą mieć dostęp wyłącznie urządzenia Dostawcy (tj. sprzęt komputerowy, w tym w szczególności: komputery osobiste, laptopy, wymienne nośniki danych) zgodne z niniejszymi wymogami i autoryzowane przez Citi.

17.47 Analiza i specyfikacja wymogów w zakresie bezpieczeństwa

Dostawca musi wdrożyć procedury w zakresie bezpieczeństwa informacji do swoich procesów i procedur dotyczących wyboru, rozwoju i wdrażania aplikacji, produktów i usług.

17.48 Transakcje internetowe

1. Jeśli to możliwe, Dostawca musi wdrożyć Systemy Informatyczne wykorzystujące dynamiczne hasła lub certyfikaty cyfrowe weryfikujące dane uwierzytelniające.
2. Wszystkie certyfikaty podmiotu końcowego należy wymieniać co najmniej raz na 13 miesięcy.
3. Aplikacje Dostawcy, które przechowują i przetwarzają informacje Citi, zarządzają nimi lub uzyskują dostęp, a także hostują aplikacje z dostępem do Internetu pod marką Citi lub mają łączność z zasobami sieciowymi Citi, muszą:
 - a. Wykorzystywać metodę uwierzytelniania opartą na typach danych/funkcji, do których uzyskiwany jest dostęp;
 - b. Spełniać wymogi oceny zgodności z uwierzytelnianiem wielopoziomowym (MFA, Multifactor Authentication) i wdrażać zalecenia zgodnie z wymogami;
 - c. Przeprowadzić ocenę wdrożenia systemu monitorowania podejrzanych działań (SAM, Suspicious Activity Monitoring) i w razie potrzeby wdrożyć zalecenia;
 - d. We wszystkich tych przypadkach Dostawca powinien skontaktować się ze swoją główną osobą do kontaktu w Citi w celu uzyskania aktualnych wymogów.

17.49 Procedury kontroli zmian

1. Dostawca musi zapewnić, że zmiany konfiguracji zapór, Systemów Wykrywania Włamań (IDS, Intrusion Detection Systems) oraz Systemów

Zapobiegania Włamaniom (IPS, Intrusion Prevention Systems) są realizowane zgodnie z procesem zarządzania zmianą po stronie Dostawcy.

2. Dostęp do środowiska produkcji za pomocą identyfikatorów tymczasowych musi być rejestrowany i podlegać nadzorowi w celu śledzenia zmian wprowadzanych w tym środowisku.
3. W przypadku Kontrolowanych Systemów Informatycznych zawierających Informacje o Kliencie sklasyfikowane przez Citi jako Poufne lub o wyższej klauzuli tajności lub o wartości składnika ryzyka systemu informatycznego dla „Integralności” lub „Dostępności” wynoszącej „Wysoki”, dzienniki przechwycone zgodnie z częścią 17.32 (Rejestrowanie wyników audytu) muszą podlegać weryfikacji przez Dostawcę. Tego typu weryfikacje mogą bazować na odpowiedniej metodologii doboru próby na podstawie ryzyka.
4. Weryfikacja musi potwierdzić, że zmiany stanowiące część tymczasowego dostępu uprzywilejowanego zostały wprowadzone zgodnie z założeniami.
5. Dostawca musi udokumentować wszystkie zmiany, w tym przechowywać dowody procesu weryfikacji.

17.50 Wyciek danych

Dostawca musi stosować udokumentowane normy bezpiecznego kodowania zapobiegające wyciekowi danych, w tym:

1. Szczegółowe informacje o systemie (np. typ serwera, parametry techniczne).
2. Ślady stosu oraz błędy wyjątku ujawniające strukturę drzewa katalogów i typ bazy danych.

17.51 Dane testowe

Informacje zdefiniowane przez Citi jako Poufne lub o wyższej klauzuli tajności nie mogą być wykorzystywane ani przechowywane przez Dostawcę w Laboratoriach, środowiskach programistycznych ani testowych, chyba że informacje te zostaną pozbawione elementów umożliwiających identyfikację, zamaskowane i/lub zaciemnione przy użyciu narzędzi i metod spełniających standardy branżowe, aby nie były już wrażliwe, albo Dostawca musi zastosować te same sposoby kontroli, jak w przypadku systemu produkcyjnego lub testowego.

17.52 Akceptowanie systemów

Dostawca musi wdrożyć udokumentowane procesy Akceptowania Systemów i Zarządzania Zakresem Projektu, które spełniają stosowne standardy branżowe.

17.53 Zgłaszanie słabych punktów dotyczących bezpieczeństwa informacji

Dostawca musi dysponować procedurą, która zapewnia, że luki w zabezpieczeniach aplikacji i infrastruktury prowadzące do utraty zasobów będących Informacjami Citi będą **natychmiast zgłaszane do Citi.**

17.54 Obowiązki i procedury dotyczące zdarzeń związanych z bezpieczeństwem

1. SIRT jest zdarzeniem związanym z bezpieczeństwem, w wyniku którego dochodzi do naruszenia któregoś z poniższych elementów, niezależnie od tego, w jaki sposób lub gdzie doszło do zdarzenia związanego z bezpieczeństwem, lub kto mógł spowodować naruszenie:

- Poufność, integralność lub dostępność danych Citi.
 - Poufność, integralność lub dostępność jakichkolwiek danych (w tym Danych osobowych), w odniesieniu do których Citi podlega zobowiązaniom umownym, prawnym lub regulacyjnym.
 - Integralność lub dostępność systemów informatycznych Citi, które przechowują, przetwarzają lub przekazują jakiekolwiek dane Citi.
2. W tym kontekście naruszenie poufności odnosi się do ujawnienia danych osobie nieupoważnionej lub do scenariuszy, w których Citi traci kontrolę nad danymi. Wszystkie zdarzenia związane z bezpieczeństwem muszą być natychmiast zgłaszane.
 3. Jeśli Dostawca doświadczył zdarzenia SIRT, musi on współpracować z Citi, dostarczając informacje wymagane przez firmę Citi zgodnie z jej własnymi procesami reagowania na zdarzenia, analizując naruszone dane w zakresie umożliwiającym Citi spełnienie wymogów prawnych, regulacyjnych lub zarządzania wewnętrznego; dokonując wszelkich zgłoszeń wymaganych przez prawo, zasady lub przepisy lub zgłoszeń wymaganych przez Citi na podstawie jej własnego uznania oraz na żądanie Citi i na koszt Dostawcy, oraz tylko po tym, jak firma Citi będzie mieć możliwość przeglądu i zmiany proponowanej treści szablonu zgłoszenia; oraz Dostawca nie może wskazać Citi w żadnych takich zgłoszeniach, chyba że Citi wyraźnie pisemnie zażąda takiego wskazania.

17.55 Ochrona przed wyciekiem danych (DLP)

Dostawca musi wdrożyć mechanizmy zapobiegania wyciekom danych (DLP, Data Leakage Prevention), między innymi monitorowanie zawartości i punktów końcowych, które obejmują wszystkich pracowników mających dostęp do danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności.

Dostawca musi wdrożyć mechanizmy kontrolne umożliwiające wykrywanie przypadków i zapobieganie przypadkom wynoszenia danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności poza swoją sieć za pośrednictwem następujących kanałów:

- a. Niezaszyfrowane wiadomości e-mail
- b. Zaszzyfrowane załączniki do wiadomości e-mail
- c. Wydruk danych Citi
- d. Przesyłanie danych Citi do lokalizacji poza siecią Citi (np. za pośrednictwem protokołu FTP)
- e. Próby kopiowania danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności na nośniki wymienne, takie jak pamięć USB, wymienne dyski twarde, napędy CD/DVD i inne urządzenia przenośne z możliwością przechowywania danych. To uprawnienie powinno być domyślnie zablokowane.
- f. Rozwiązanie DLP musi być oparte na wprowadzaniu rejestrów i ostrzeganiu Dostawcy o wszystkich zdarzeniach, które stanowią

- próby (zakończone powodzeniem lub zablokowane)
przemieszczania, przesyłania lub kopiowania danych Citi
sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności z sieci
Citi do innych miejsc docelowych. To uprawnienie powinno być
domyślnie zablokowane.
- g. Wczytywanie danych Citi do zewnętrznych witryn internetowych,
w tym witryn SaaS lub umożliwiających udostępnianie plików. To
uprawnienie powinno być domyślnie zablokowane.

17.56 Przeglądanie stron internetowych

1. Dostawca musi dysponować mechanizmami kontroli dostępu do sieci, aby zapobiec udostępnianiu danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności oraz narażeniu pracowników mających dostęp do danych Citi na działanie złośliwego oprogramowania lub ataki.
2. W przypadku Dostawców, którzy mają dostęp do danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności:
 - a. Wszystkie żądania adresów URL muszą być rejestrowane.
 - b. Próby uzyskania dostępu do stron, które mogą zostać wykorzystane do nieautoryzowanego udostępniania danych Citi (np. poprzez pocztę internetową, chat, media społecznościowe, pamięć masową online, generatywną sztuczną inteligencję itp.), muszą być blokowane.
 - c. Dostęp do stron, które mogą narazić środowisko na działanie złośliwego oprogramowania lub atak, musi być blokowany.
 - d. Próby uzyskania dostępu do stron uznanych za niepowiązane z działalnością biznesową muszą być blokowane.
 - e. Dostawca musi mieć wykupioną usługę kategoryzacji adresów URL, która jest regularnie aktualizowana; wszystkie nieskategoryzowane adresy URL muszą być domyślnie blokowane albo wszystkie adresy URL muszą być domyślnie blokowane i zatwierdzane indywidualnie w każdym przypadku.
 - f. Przeglądarki internetowe używane przez Dostawcę muszą posiadać pełne wsparcie i najnowsze aktualizacje zabezpieczeń dostarczane przez dostawcę oprogramowania.

17.57 Wiadomości elektroniczne

Do przesyłania lub przechowywania Informacji Citi poza siecią Dostawcy lub z sieci zawierających Informacje Citi nie należy wykorzystywać komunikatorów, sieci peer-to-peer ani internetowych narzędzi do współpracy, chyba że stosuje się odpowiednie szyfrowanie wszystkich danych Citi zgodnie z punktem 17.9 (Polityka dotycząca korzystania z kryptograficznych środków kontroli).

17.58 Poczta e-mail

Dostawca musi stosować mechanizmy kontroli poczty elektronicznej zapobiegające udostępnianiu Informacji Citi i narażeniu ich na złośliwe oprogramowanie lub atak. Obejmuje to:

1. Skanowanie i blokowanie załączników przychodzących do bramki pocztowej, jeśli stanowią zagrożenie dla systemu.

2. Korzystanie z maksymalnie aktualnego oprogramowania do filtrowania poczty elektronicznej (Anti-Spam, Anti-Phishing).
3. Szyfrowanie wszelkich danych Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności w przypadku wysyłania ich poza organizację Dostawcy.
4. Pełną obsługę klientów poczty elektronicznej używanych przez Dostawcę i zapewnienie im najnowszej aktualizacji zabezpieczeń dostarczonych przez dostawcę oprogramowania.

17.59 Nośniki wymienne

1. Dostawca musi chronić Informacje Citi niezależnie od nośnika, na którym się one znajdują. Ten standard dotyczy między innymi następujących rodzajów nośników: karta, kasetę, płyta kompaktowa (CD), blankiet czekowy, dyskietka lub inne wymienne urządzenie pamięci masowej, wydruk papierowy, dysk magnetyczny, taśma magnetyczna, mikrofilm, mikrofisz, dysk optyczny lub dokument papierowy.
2. Domyślnym ustawieniem dostępu do przenośnych nośników / urządzeń pamięci masowej w systemach, w których przechowywane są Informacje Citi, musi być opcja braku dostępu. Jeśli dopuszcza się wyjątki i przydziela dostęp umożliwiający odczytywanie i zapisywanie danych, dane na nośniku przenośnym należy zaszyfrować.
3. Jeżeli dozwolone jest korzystanie z nośników wymiennych, musi ono podlegać procesowi zatwierdzenia przez kierownictwo wraz z uzasadnieniem biznesowym wskazującym na konieczność korzystania z nośnika wymiennego. Nośniki wymienne muszą być inwentaryzowane przez kierownictwo. Nośniki wymienne zawierające dane Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności muszą być automatycznie szyfrowane bez konieczności podejmowania jakichkolwiek działań przez użytkownika.

17.60 Utylizacja nośników

1. Jeśli Informacje Citi sklasyfikowane przez Citi jako Poufne lub o wyższej klauzuli tajności kwalifikują się do zniszczenia zgodnie z instrukcjami przekazanymi przez Citi (tj. w momencie, w którym takie informacje nie są już wymagane przez Citi ani użyteczne dla Citi oraz po upływie każdego dodatkowego okresu przechowywania informacji wymaganego przez prawo i/lub wygaśnięcia polityki Citi), Dostawca musi zniszczyć takie informacje w sposób, który sprawi, że ich odzyskanie lub użytkowanie nie będzie już możliwe.
2. W celu bezpiecznego usuwania danych przechowywanych na nośnikach należy użyć zatwierdzonego narzędzia, które losowo nadpisuje sektory dysku określonym zestawem różnych znaków, zgodnie z poniższymi zasadami:
 - a. W przypadku nośników, na których przechowywane są Informacje poufne lub o wyższej klauzuli tajności, narzędzie musi trzykrotnie wykonać procedurę nadpisywania danych na nośnikach.
 - b. Należy trwale i skutecznie zniszczyć dane narzędziem demagnetyzującym typu degausser (jeśli ma to zastosowanie).

3. Należy zniszczyć nośnik fizycznie, aby uniemożliwić jego odczytanie (np. przecięcie, zgniatanie dysków).
4. Papierowe i inne nieelektroniczne nośniki zawierające Informacje poufne lub o wyższej klauzuli tajności muszą być bezpiecznie zbierane i przechowywane w zabezpieczonym Pojemniku na informacje poufne przed ich ostateczną utylizacją. Pojemniki na informacje poufne muszą być zawsze zamknięte, a ich otwarcie może być możliwe tylko przez upoważniony personel.
 - a. Kserokopiarki, drukarki, faksy i wszelkie inne urządzenia, w których pamięci mogą znajdować się dane Citi sklasyfikowane jako Poufne lub o wyższej klauzuli tajności, również muszą zostać poddane sanityzacji.

17.61 Zarządzanie bezpieczeństwem informacji i szkolenia

1. Prowadzenie odpowiedniego programu edukacyjnego w zakresie bezpieczeństwa cybernetycznego/informacji, który obejmuje m.in. zapobieganie phishingowi i innym atakom wykorzystującym inżynierię społeczną, odpowiednie postępowanie z informacjami poufnymi lub o wyższej klauzuli tajności oraz zgłaszanie zdarzeń związanych z bezpieczeństwem i reagowaniem na zdarzenia.
2. Dostawca zobowiązany jest zapewnić wszystkim pracownikom, w tym wykonawcom i pracownikom tymczasowym, odpowiednią edukację i szkolenia z zakresu polityk i procedur organizacyjnych istotnych dla ich stanowiska pracy.
3. Dostawca zobowiązany jest zapewnić, że program szkoleń i edukacji w zakresie podnoszenia świadomości jest poddawany corocznemu przeglądowi i aktualizowany w celu uwzględnienia pojawiających się ryzyk i zagrożeń, bieżących najlepszych praktyk oraz nowych technologii w obszarze cyberbezpieczeństwa.
4. Należy uwzględnić co najmniej następujące tematy:
 - b. Oznaczanie informacji i postępowanie z nimi
 - c. Bezpieczne przesyłanie danych (bezpieczna poczta elektroniczna, bezpieczne przechowywanie danych na platformie SharePoint, niewysyłanie danych należących do Citi na prywatną pocztę elektroniczną)
 - d. Zgłaszanie incydentów związanych z bezpieczeństwem informacji
 - e. Bezpieczne miejsce pracy (np. odpowiednie korzystanie z Internetu, nieautoryzowane oprogramowanie, zakaz pobierania niezatwierdzonego oprogramowania)
 - f. Zarządzanie hasłami (np. silne hasła, zakaz udostępniania haseł)
 - g. Inżynieria społeczna (np. phishing, spear fishing, vishing, SMishing)
 - h. Praca zdalna (np. bezpieczne połączenie, bezpieczeństwo urządzeń osobistych)
5. Pracownicy dostawcy muszą zostać przydzieleni do szkolenia po otrzymaniu lub przed otrzymaniem dostępu do systemów hostujących dane Citi i ukończyć szkolenie przed upływem terminu wskazanego w powiadomieniu o przypisaniu szkolenia.
 - a. Szkolenia w zakresie bezpieczeństwa informacji powinny być prowadzone dla całego personelu co najmniej raz w roku, o ile nie jest to zabronione przez prawo.
6. Szkolenie powinno obejmować artefakt do udokumentowania oceny jego efektywności (tj. test po zakończeniu z progiem zaliczenia), gdzie lokalne prawo na to zezwala.

17.62 Program zarządzania ryzykiem cybernetycznym

Dostawca musi również stosować co najmniej odpowiedni program zarządzania ryzykiem cybernetycznym, który obejmuje co najmniej:

1. Utrzymywanie dobrze zdefiniowanego, udokumentowanego programu zarządzania ryzykiem w zakresie bezpieczeństwa informacji i/lub programu

zarządzania ryzykiem operacyjnym, który ma jasno zdefiniowany element zarządzania ryzykiem cybernetycznym/informacyjnym, określającym gotowość Dostawcy na ryzyko cybernetyczne i zapewniającym, że jego cybernetyczne ryzyko szczytkowe będzie dostosowane do tej gotowości.

2. Utrzymywanie solidnego programu zarządzania ryzykiem w zakresie bezpieczeństwa, który obejmuje, ale nie ogranicza się do gromadzenia i/lub przeprowadzania audytów i przeglądów bezpieczeństwa, które oceniają ogólny stan bezpieczeństwa w organizacji oraz składania kierownictwu wykonawczemu co najmniej raz w roku raportu w celu przeglądu i zapewnienia, że gotowość Dostawcy na ryzyko cybernetyczne nie została naruszona.
3. Utrzymywanie zgodności ze standardami bezpieczeństwa danych PCI (PCI-DSS, PCI Data Security Standards) mającymi zastosowanie do Dostawcy, gdy Dostawca przetwarza, przechowuje i/lub przesyła transakcje kartą kredytową/debetową, płatności i/lub informacje.
4. Utrzymywanie planu zarządzania kryzysowego oraz podręcznika i planu Security Incident Response Team (SIRT) zgodnego ze standardami branżowymi, aby zapewnić, że Dostawca ma wystarczającą i odpowiednią zdolność do wykrywania, zabezpieczania, sprawdzania, reagowania i odzyskiwania sprawności po wszelkich próbach lub podejrzeniach naruszeń bezpieczeństwa cybernetycznego i/lub rzeczywistych przypadkach naruszenia bezpieczeństwa cybernetycznego.

17.63 Bezpieczeństwo aplikacji, API, kodu, systemu i infrastruktury

Jeśli Dostawca hostuje, rozwija, współtworzy, udostępnia środowiska programistyczne i/lub dostarcza (a) aplikacje, Dostawca dokona przeglądu kodu wspomnianego oprogramowania i/lub poprawek do oprogramowania pod kątem luk w zabezpieczeniach, zapobiegania nieautoryzowanemu dostępowi, modyfikacji i/lub wstawiania złośliwego oprogramowania lub innych form złośliwego kodu oraz testowania luk w zabezpieczeniach w celu zapewnienia, że aplikacja (w tym interfejsy API) oraz podstawowe usługi systemowe, systemy operacyjne i sieci są wolne od znanych luk i usterek, które mogą skutkować zdarzeniem związanym z bezpieczeństwem, naruszeniem prywatności, oszustwem, nieautoryzowanym dostępem i/lub ujawnieniem Informacji poufnych, utratą integralności informacji przetwarzanych, przechowywanych lub przesyłanych przez aplikację (aplikacje) i/lub utratą dostępności, która może wpłynąć na jakość produktów i/lub usług, które Dostawca dostarcza Citi.

17.64 Bezpieczeństwo urządzeń mobilnych

Jeśli Dostawca zapewnia rozwiązanie w zakresie aplikacji mobilnych, musi przestrzegać następujących wymogów:

1. Aplikacja mobilna musi obsługiwać tylko ogólnie dostępne (GA), stabilne, niewycofane wersje² systemu Google Android (z wyjątkiem Android Go) i/lub

² Wersje produktu, które są aktywnie obsługiwane i otrzymują regularne aktualizacje zabezpieczeń od właściciela platformy lub Dostawcy.

platform Apple iOS / iPadOS. Jeśli rozwiązanie mobilne obsługuje dodatkowe systemy lub wersje, Citi musi mieć możliwość konfiguracji tych obsługiwanych systemów operacyjnych / wersji.

2. Rozwiązanie mobilne nie powinno obsługiwać platform / urządzeń mobilnych, które nie są wyposażone w regularne zestawy instrukcji do obsługi algorytmów kryptograficznych, w tym, między innymi, metod szyfrowania określonych w Części 17.9 (Wymagania dotyczące szyfrowania) niniejszego dokumentu.
3. W środowisku produkcyjnym nie są dozwolone żadne wersje systemu operacyjnego w fazie przedprodukcyjnej, w tym między innymi wersje beta, wersje z wczesnym dostępem i wersje poglądowe / wydania z nowymi funkcjami.
4. Dostawca musi być w stanie dostarczyć listę zintegrowanych komponentów stron trzecich, w tym, między innymi, bezpłatne i otwarte biblioteki oprogramowania, które są pakietowane/zarządzane przez rozwiązanie mobilne.
5. Aplikacja mobilna musi być zgodna z wymaganiami i najlepszymi praktykami, które przewidują publikowanie aplikacji mobilnych za pośrednictwem publicznych sklepów z aplikacjami, takich jak Apple App Store lub Google Play. Preferowaną i podstawową metodą dystrybucji/publikowania aplikacji mobilnych będą wymienione publiczne sklepy z aplikacjami.
6. Aplikacje mobilne Android muszą korzystać ze schematu podpisów APK v2+. Nie można używać schematu podpisywania APK w wersji 1 (zwanego też podpisywaniem JAR).
7. Typ i długość klucza do podpisywania aplikacji mobilnych muszą być zgodne z częścią 17.9 — Wymagania dotyczące **szyfrowania** znajdującą się w niniejszym dokumencie.
8. Każdy klucz podpisywania aplikacji i powiązany certyfikat X.509v3 muszą być zarządzane indywidualnie i przypisane do konkretnego identyfikatora aplikacji / identyfikatora pakietu. Klucze podpisywania nie mogą być współdzielone między aplikacjami.
9. Jeśli aplikacja mobilna wymaga przechowywania danych na urządzeniu mobilnym, musi przechowywać na urządzeniu wyłącznie najnowsze dane, które są niezbędne do celów aplikacji/usługi lub tak długo, jak jest to wymagane zgodnie z wymogami prawnymi lub regulacyjnymi.
 - a. Gromadzenie, przetwarzanie i/lub przechowywanie danych użytkowników musi być zgodne z lokalnymi przepisami, między innymi z przepisami dotyczącymi prywatności, takimi jak Ogólne rozporządzenie o ochronie danych (RODO) i dyrektywa 2002/58/WE (o e-prywatności) lub ich regionalne odpowiedniki.
 - b. Zintegrowane komponenty stron trzecich (np. biblioteki) nie mogą gromadzić, przetwarzać ani przechowywać danych użytkownika.
10. Aplikacje mobilne nie mogą umożliwiać ogólnodostępnego dostępu do żadnych danych aplikacji.
 - a. Jeśli wymagane jest udostępnianie danych innym aplikacjom, aplikacje muszą wykorzystywać komercyjnie uzasadnione techniki,

metody i mechanizmy kontroli dotyczące odpowiednich systemów operacyjnych, tak by udostępniać tylko niezbędną ilość danych minimalnej liczbie innych aplikacji, w przypadku których takie udostępnianie danych jest odpowiednio uzasadnione i dokumentowane.

11. Aplikacje mobilne muszą polegać wyłącznie na bezpiecznych funkcjach komunikacji zapewnianych przez odpowiednie mobilne systemy operacyjne.
Np.
 - a. Aplikacje na system Android muszą w swoim manifestie aplikacji i/lub pliku konfiguracji sieci wyraźnie deklarować, że niezabezpieczony ruch sieciowy nie jest dozwolony względem żadnej domeny sieciowej.
 - b. Aplikacje na systemy iOS/iPadOS muszą bez żadnego wyjątku korzystać z zestawu zabezpieczeń Application Transport Security (ATS).
12. Materiały kryptograficzne powinny być powiązane ze sprzętowo zabezpieczonym magazynem kluczy.
13. Aplikacje mobilne muszą być tworzone w trybie wersji gotowej do publikacji i nie mogą zawierać:
 - a. Żadnej funkcji ani metody, która może umożliwiać pominięcie środków kontroli bezpieczeństwa,
 - b. Informacji dotyczących debugowania, takich jak nazwy plików kodu źródłowego, nazwy zmiennych, nazwy symboli, komentarzy itp., które mogą ułatwić inżynierię wsteczną.
14. Aplikacje mobilne muszą korzystać ze skutecznych mechanizmów zapobiegających hookingowi lub manipulacjom, aby zapobiegać wstrzykiwaniu złośliwego kodu, który mógłby zmieniać lub monitorować zachowanie aplikacji w czasie wykonywania.
15. Aplikacje mobilne muszą wykorzystywać kompleksowe techniki zapobiegające debugowaniu lub inżynierii wstecznej / zaciemnianiu kodu, aby utrudnić ataki inżynierii wstecznej.
16. Pakiety aplikacji mobilnych muszą oferować możliwość weryfikacji autentyczności i integralności ich zawartości (np. przy użyciu kryptograficznej sumy kontrolnej i/lub podpisu cyfrowego).
17. Jeśli aplikacja mobilna wymaga uwierzytelnienia użytkownika, kontrole integralności aplikacji i/lub urządzenia powinny zostać zakończone przed rozpoczęciem uwierzytelniania użytkownika.
18. Aplikacje mobilne, które uzyskują dostęp do wszelkich informacji będących własnością Citi, sklasyfikowanych przez Citi jako Poufne lub o wyższej klauzuli tajności i/lub o klasyfikacji ryzyka związanego z bezpieczeństwem informacji na poziomie średnim lub o wyższej klauzuli tajności, lub też takie informacje przetwarzają je lub przechowują, muszą wykorzystywać wyłącznie silne metody biometryczne (np. spełniać lub przewyższać kategorię Klasy 3 / Silne, jak określono w odpowiednim [Android Compatibility Definition Document](#)).

19. Aplikacje mobilne muszą wdrożyć środki przeciwdziałające atakom typu Man-in-the-middle (MitM).
20. Aplikacje mobilne muszą być w stanie wykrywać zagrożone urządzenia, w tym między innymi urządzenia mobilne z zainstalowanym „jailbreakiem” lub „zrootowane” oraz reagować na nie zgodnie z oceną ryzyka biznesowego i wymogami regulacyjnymi.
21. Aplikacje mobilne muszą wykorzystywać silne powiązanie z urządzeniem, aby zapobiec klonowaniu tokenu oprogramowania (np. dowodu posiadania).
22. Aplikacje mobilne muszą korzystać z bezpiecznych aplikacji / rozwiązań klawiaturowych (np. takich, które są wbudowane / wstępnie zainstalowane przez mobilne systemy operacyjne).
23. Powiadomienia push nie mogą zawierać żadnych poufnych informacji (np. informacji Citi sklasyfikowanych jako Poufne lub o wyższej klauzuli tajności). Za pomocą powiadomienia typu „push” można jednak rozsyłać hasła jednorazowe (OTP).
24. Rozwiązania z zakresu aplikacji mobilnych muszą umożliwiać odrzucanie/ignorowanie prób komunikacji z klientami używającymi wersji aplikacji ze znanymi lukami bezpieczeństwa.
25. Aplikacje mobilne muszą być zgodne z najlepszymi praktykami branżowymi, między innymi z technikami zapobiegania opublikowanymi w dokumencie [OWASP Mobile Top 10](#).
26. Aplikacje mobilne wykorzystujące sztuczną inteligencję i techniki uczenia maszynowego (AI/ML) muszą to robić etycznie i zgodnie z częścią 19 — **Error! Reference source not found.** (włączając generatywną sztuczną inteligencję / Agentic AI).
27. Aplikacja mobilna musi stosować minimalne uprawnienia urządzenia, które są wymagane do realizacji celów/funkcji wykorzystywanych przez Citi.
28. Aplikacje mobilne nie mogą przechowywać żadnych niepublicznych informacji na zewnętrznych/wymiennych nośnikach pamięci, takich jak karty SD. **Error! Reference source not found.**

17.65 Ujawnienie informacji o oprogramowaniu

Dostawca ujawni wszelkie komponenty oprogramowania, w tym m.in. oprogramowanie typu open source zawarte w produktach lub usługach świadczonych na rzecz Citi (łącznie „Komponenty oprogramowania”). Dostawca nie będzie aktualizować, uaktualniać ani w inny sposób włączać Komponentów oprogramowania do jakiegokolwiek wersji produktów lub usług, która ma zostać zainstalowana w Systemach Citi, bez uprzedniego każdorazowego poinformowania o tym fakcie Citi. Ponadto Dostawca ma obowiązek dopilnować, aby jego produkty lub usługi nie zawierały Komponentów oprogramowania, które jest licencjonowane na warunkach nakładających na firmę Citi lub jej Podmioty powiązane jakiejkolwiek zobowiązania, które nie zostały wyraźnie ujawnione i zaakceptowane przez Citi w Umowie. Dostawca ujawni Citi wszelkie złośliwe Komponenty oprogramowania wykryte w organizacji, produktach lub usługach Dostawcy w ciągu 30 dni od ich wykrycia. W szczególności Dostawca ujawni fakt korzystania przez niego z Komponentów oprogramowania w dowolnej wersji produktów lub usług, przekazując Citi dokument z zestawieniem materiałów oprogramowania (SBOM,

Software Bill of Materials) w formacie pliku OWASP CycloneDX lub w formacie pliku specyfikacji ISO/IEC 5962:2021 Software Package Data Exchange (SPDX). Takie ujawnienie informacji musi obejmować źródło pochodzenia Komponentów oprogramowania (np. dostawca komercyjny, wbudowana baza danych, publiczny binarny menedżer pakietów, oprogramowanie zbudowane z kodu źródłowego, dostawca oprogramowania open source lub dowolne Oprogramowanie wbudowane, lub wyselekcjonowany dostawca Komponentów oprogramowania) oraz informację, czy Dostawca lub którykolwiek z jego podmiotów zależnych w łańcuchu dostaw oprogramowania pobrał kopię Komponentów oprogramowania (znaną jako „fork”), a następnie wbudował ją w swoje produkty lub usługi jako zależność pakietu lub jako kod źródłowy zintegrowany z kodem źródłowym Dostawcy, z którego kompilowane są produkty i usługi.

17.66 Modelowanie zagrożeń

Dostawca musi wdrożyć proces modelowania zagrożeń, który kompleksowo uwzględnia i/lub obejmuje wszystkie poniższe elementy:

1. Definicja zakresu: Dostawca musi jasno określić zakres modelu zagrożeń, koncentrując się na komponentach oprogramowania i przepływach danych, które przetwarzają, przechowują lub przekazują Informacje Citi sklasyfikowane jako Poufne i o wyższej klauzuli tajności.
2. Identyfikacja zagrożenia: Dostawca musi systematycznie identyfikować potencjalne zagrożenia i luki w zabezpieczeniach dotyczące projektu, architektury i przeznaczenia oprogramowania, biorąc pod uwagę różne wektory ataków i podmioty zagrażające bezpieczeństwu na wczesnym etapie cyklu życia projektu.
3. Analiza ryzyka: Dostawca musi analizować zidentyfikowane zagrożenia w celu oceny ich potencjalnego wpływu i prawdopodobieństwa, umożliwiając priorytetyzację zagrożeń bezpieczeństwa.
4. Integracja mechanizmów kontroli: Dostawca musi określić i zintegrować odpowiednie środki kontroli bezpieczeństwa oraz strategie ograniczania ryzyka w projekt i proces rozwoju oprogramowania, aby reagować na te priorytetowe zagrożenia.
5. Dokumentacja: Dostawca musi udokumentować model zagrożeń, w tym zidentyfikowane zagrożenia, związane z nimi ryzyko i odpowiednie wdrożone środki zaradcze.
6. Przegląd okresowy: Dostawca musi regularnie weryfikować i aktualizować modele zagrożeń, zwłaszcza gdy występują istotne zmiany w projekcie oprogramowania, funkcjach lub środowisku wdrożeniowym.

17.67 Sztuczna inteligencja

1. Dostawcy muszą wdrożyć solidny bezpieczny cykl życia wytwarzania oprogramowania (SSDLC, Secure Software Development Lifecycle) dla wszystkich systemów i komponentów AI/ML dostarczonych lub zintegrowanych z Citi. Obejmuje to bezpieczne projektowanie, rozwój, testowanie, wdrażanie i bieżące utrzymywanie oprogramowania.

2. Systemy sztucznej inteligencji dostarczane przez Dostawcę muszą wykazywać integralność działania i dużą odporność na ataki kontrybucyjne. Obejmuje to wdrożenie mechanizmów wykrywania ataków typu prompt injection (wstrzykiwania złośliwych poleceń), sanityzację danych wejściowych i utrzymywanie izolacji danych.
3. Agenci i komponenty sztucznej inteligencji dostarczane przez dostawców muszą bezpiecznie wchodzić w interakcje z systemami i innymi narzędziami Citi. Wymaga to silnych mechanizmów zarządzania tożsamością i dostępem, rygorystycznej walidacji argumentów wywoływania narzędzia oraz izolacji operacji z wykorzystaniem narzędzi wysokiego ryzyka. Mechanizmy Human-in-the-Loop (HITL) muszą być stosowane w przypadku działań wrażliwych lub wysokiego ryzyka.
4. Systemy sztucznej inteligencji Dostawcy muszą generować kompleksowe, trwałe i umożliwiające audyt dzienniki wszystkich istotnych zdarzeń. Dzienniki te muszą być chronione przed manipulacją, agregowane i przechowywane zgodnie z politykami Citi. Funkcje ciągłego monitorowania i wykrywania anomalii są wymagane do identyfikacji oraz zgłaszania zdarzeń i podejrzanych działań związanych z bezpieczeństwem.
5. Systemy sztucznej inteligencji Dostawcy muszą umożliwiać ludzki nadzór oparty na analizie ryzyka, umożliwiając odpowiednią interwencję, i być zaprojektowane z jasno określoną odpowiedzialnością za wyniki i działania sztucznej inteligencji. Obejmuje to klasyfikację wyników AI według poziomu ryzyka i zapewnienie możliwości ich nadpisywania przez człowieka.
6. Wszyscy agenci, komponenty i systemy sztucznej inteligencji dostarczane przez dostawców muszą wdrażać solidne środki kontroli tożsamości i zarządzania dostępem. Każda interakcja AI musi być przypisana do możliwej do zidentyfikowania tożsamości (ludzkiej lub maszynowej), a każdy dostęp wymaga uwierzytelniania. Agenci sztucznej inteligencji muszą używać tożsamości zarządzanych i przestrzegać zasad jak najmniejszych uprawnień podczas dostępu do zasobów Citi.
 - a. Dostawcy muszą zagwarantować, że wszystkim agentom AI przydzielono tożsamości agenta w ramach sieci identyfikacji obiektów Citi (COIN, Citi Object Identity Network), sfederowane z systemami zarządzania tożsamością i dostępem Citi (IAM, Identity and Access Management), aby umożliwić stosowanie polityk bezpieczeństwa Citi, scentralizowane zarządzanie tożsamością i audytowalność.
 - b. Dostawcy muszą wdrożyć agentów stron trzecich do COIN przy użyciu zatwierdzonych przez Citi mechanizmów integracji, w tym interfejsu API COIN udostępnianego za pośrednictwem bezpiecznych bram (takich jak SSG Gateway lub Apigee), i muszą zapewnić, że takie wdrożenie jest przeprowadzane w bezpieczny sposób zgodnie z obowiązującymi wymogami Citi w zakresie bezpieczeństwa.
 - c. Dostawcy, jeśli są hostowani wewnętrznie, muszą generować własny token zgodny z COIN; Dostawcy hostowani zewnętrznie i uwierzytelniający ruch przychodzący własnym tokenem federacyjnym muszą mieć obsługiwany token wymiany dla tokenów

Citi, np. wymiana z MSFT na tokeny COIN. Każdy nowy typ tokenu, który nie jest obecnie obsługiwany poprzez wymianę, musi zostać sprawdzony i zatwierdzony przez zespół IAM w Citi.

7. Jeśli dostawcy wykorzystują lub dostarczają serwery lub klientów Model Context Protocol (MCP), muszą wdrożyć MCP RFC 7591, w tym wszystkie opcjonalne funkcje.
8. Systemy sztucznej inteligencji dostawców muszą chronić monity systemowe i wewnętrzne mechanizmy przed ujawnieniem lub manipulacją. Zarządzanie kontekstem musi egzekwować ściśle granice, aby zapobiec wyciekowi danych między klientami, użytkownikami lub środowiskami.
9. Dostawcy muszą mieć udokumentowane procedury wykrywania incydentów bezpieczeństwa związanych ze sztuczną inteligencją — w tym ataków kontrykcyjnych, manipulacji modelami, nieautoryzowanych działań związanych ze sztuczną inteligencją lub naruszeń danych obejmujących systemy sztucznej inteligencji — jak również reagowania na te incydenty i zgłaszania ich. Należy niezwłocznie powiadomić Citi o wszelkich takich incydentach.

18 WYTYCZNE DOTYCZĄCE BEZPIECZNEGO MIEJSCA PRACY

Dotyczy dostawców, którzy uzyskują dostęp do informacji Citi, przetwarzają je, zarządzają nimi i przechowują je ORAZ/LUB hostują aplikacje Citi z dostępem do Internetu ORAZ/LUB mają dostęp do zasobów sieciowych Citi ORAZ/LUB wymagają dostępu bez nadzoru do obiektów Citi.

Dostawcy muszą chronić środki trwałe oraz wartości niematerialne i prawne firmy Citi i jej Klientów. Aktywa Citi i Klientów można wykorzystywać w zatwierdzonych celach i w zatwierdzony sposób (np. zgodnie z odpowiednimi licencjami oraz warunkami), wyłącznie w odniesieniu do celów biznesowych Citi oraz Dostawców Citi. Aktywa obejmują gotówkę, papiery wartościowe, majątek fizyczny, usługi, plany biznesowe, Informacje Citi, informacje Dostawcy, informacje dystrybutorów, własność intelektualną (programy komputerowe, modele i inne elementy) oraz wszystkie inne dane osobowe, informacje zastrzeżone i Informacje poufne. Sprzeniewierzenie lub nieupoważnione ujawnienie aktywów Citi stanowi naruszenie obowiązków wobec Citi i może też być traktowane jako nadużycie wobec Citi. Podobnie nieupoważnione użytkowanie, marnotrawstwo lub niedbałość w odniesieniu do aktywów Citi stanowi naruszenie obowiązków wobec Citi.

Pozycja	Wymogi
Informacje Citi (dokumentacja elektroniczna i papierowa)	Informacje Citi należy umieszczać i przechowywać w zamkniętym, odpowiednio zabezpieczonym miejscu po zakończeniu normalnego dnia pracy i zawsze, gdy Dostawca znajduje się z dala od wyznaczonego miejsca pracy.

Pozycja	Wymogi
Komputery stacjonarne i laptopy	Komputery i laptopy wykorzystywane do uzyskiwania dostępu do Informacji Citi lub ich przeglądania muszą być zabezpieczone poprzez ustawienie wygaszacza ekranu, który włącza się po upływie okresu bezczynności i wymaga podania hasła. Za każdym razem, gdy Dostawca oddala się od wyznaczonego miejsca pracy, musi zablokować komputer i/lub laptop za pomocą kombinacji klawiszy CTRL + ALT + DEL i wybrać opcję „Zablokuj komputer”. Jeśli Dostawca wykorzystuje laptopa do przeglądania Informacji Citi, musi on dopilnować, aby w trakcie godzin pracy taki laptop był przymocowany do jednostki podstawowej za pomocą linki zabezpieczającej lub zamka, a po zakończeniu zwykłych godzin pracy — zamknięty w bezpiecznym miejscu.
Zamknięcie na klucz	Po upływie normalnych godzin pracy należy zamknąć szafki na akta oraz szuflady, w których przechowywane są Informacje Citi.
Otwarte przestrzenie biurowe	Otwartych powierzchni biurowych nie wolno używać jako serwerów plików / mini centrów danych do przechowywania Informacji Citi, chyba że zostały specjalnie zaprojektowane do takiego użytku i udokumentowane przez Citi.
Drukarki, kserokopiarki i tace odbiorcze do faksu	Należy usunąć wszystkie materiały związane z Citi z drukarek, kserokopie i faksów.
Utylizacja	Należy usuwać Informacje Citi, które nie są już potrzebne (zgodnie ze stosownymi harmonogramami przechowywania materiałów). Dokumenty należy zniszczyć w niszczarce lub umieścić w bezpiecznym/zamykanym koszu na odpady. Po prawidłowym przeprowadzeniu procedur w zakresie usuwania danych z nośników elektronicznych i magnetycznych nośniki takie należy zutylizować w bezpieczny sposób.

19 SZTUCZNA INTELIGENCJA / UCZENIE MASZYNOWE (W TYM GENERATYWNA SZTUCZNA INTELIGENCJA / AGENTIC AI)

Dotyczy Dostawców, którzy wykorzystują sztuczną inteligencję / uczenie maszynowe (AI/ML, Artificial Intelligence / Machine Learning), w tym generatywną sztuczną inteligencję / Agentic AI, zgodnie z definicją Citi w niniejszych Wymaganiach dla Dostawców, w dowolnej części produktu lub świadczonej usługi.

19.1 Dostawca nie będzie wykorzystywał — i musi zapewnić, że żaden Podwykonawca nie wykorzystuje — opisanych poniżej rozwiązań AI/ML, chyba że takie wykorzystanie zostało uzgodnione między Stronami w odpowiednim Harmonogramie lub Zleceniu pracy w ramach Umowy:

- a. Używane, zawarte lub w inny sposób włączone do jakiegokolwiek produktu lub usługi, w odniesieniu do których jest objęte Umową bezpośredniego lub pośredniego dostarczenia Citi, lub w jakiegokolwiek jego części, w tym zawartego lub osadzonego w produkcie lub usłudze strony trzeciej; lub
2. Wykorzystywane w jakikolwiek sposób podczas wykonywania przez Dostawcę dowolnej Umowy, niezależnie od tego, czy takie rozwiązanie AI/ML jest wykorzystywane, zawarte lub w inny sposób włączone do produktu lub usługi dostarczanej Citi; lub
3. Wykorzystywane przez Dostawcę w sposób, który może narazić Informacje Citi na kontakt z takim rozwiązaniem AI/ML, w tym m.in. rozwiązaniem AI/ML wykorzystywanym przez Dostawcę w jego niekomercyjnej działalności biznesowej (np. prowadzeniu dokumentacji biznesowej, usprawnianiu procesów, badaniach i rozwoju, zachowaniu zgodności i audycie wewnętrznym).

19.2 Nieprzestrzeganie przez Dostawcę tych zobowiązań uznaje się za istotne naruszenie warunków niniejszej Umowy.

19.3 Na żądanie organu regulacyjnego, w ramach jakiegokolwiek inspekcji dozorowej lub dochodzenia sądowego dotyczącego stosowania rozwiązań AI/ML w jakiegokolwiek części produktu/usługi, Dostawca musi pomóc Citi w odpowiedzi na żądanie organu regulacyjnego, w tym przeprowadzić i/lub ułatwić przeprowadzanie audytów algorytmów niezbędnych do poznania rzeczywistych działań algorytmów wchodzących w skład modeli AI/ML.

19.4 Należy również przestrzegać następujących zasad:

Zgodność z prawem. Dostawca AI/ML jest zobowiązany do przestrzegania Obowiązującego prawa.

Cel i proporcjonalność. Dostawca nie będzie łączyć Treści ani Informacji Citi z Dostawcą ani żadnymi danymi stron trzecich. Dostawca nie będzie wykorzystywać Treści ani Informacji Citi do szkolenia AI/ML bez pisemnej zgody Citi. Dostawca AI/ML nie będzie korzystać z Treści ani Informacji Citi, z wyjątkiem zakresu wymaganego do świadczenia Usług.

20 SKARGI KLIENTÓW

20.1 Skarga to ustna lub pisemna komunikacja, która może zostać przekazana ustnie (osobiście lub telefonicznie) lub na piśmie (poprzez pocztę lub komunikację elektroniczną, taką jak poczta e-mail, czat lub media społecznościowe itp.). Wyraża niezadowolenie Klienta, osoby niebędącej Klientem, klienta Citi, potencjalnego Klienta lub autoryzowanego przedstawiciela Klienta (łącznie określani mianem „Klienta”) z Polityki Citi, produktu lub usługi oferowanych przez Citi lub za

pośrednictwem Citi, pracownika Citi, wykonawcy Citi lub usługodawcy zewnętrznego działającego w imieniu Citi lub dowolnej kombinacji powyższych.

- 20.2** Dostawcy muszą przestrzegać Polityki postępowania ze skargami klientów Citi, a także wszelkich obowiązujących Standardów i Procedur Citi związanych ze skargami. Dostawca w ciągu dwudziestu czterech (24) godzin powiadomi na piśmie odpowiednią główną osobę kontaktową w Citi (lub osobę wyznaczoną) o każdym pisemnym lub ustnym zgłoszeniu niezadowolenia lub zastrzeżenia (każde z nich zwane dalej „Skargą”) otrzymanym przez Dostawcę od dowolnego Klienta (lub osoby niebędącej Klientem lub potencjalnego Klienta, zgodnie z definicją Skargi Citi) lub od dowolnego Organu regulacyjnego w związku z Usługami świadczonymi przez Dostawcę w imieniu Citi lub w inny sposób związanego z Citi. O ile Citi nie udostępni takiego systemu Dostawcy, Dostawca zobowiązany jest również do opracowania, wdrożenia i utrzymywania systemu („System monitorowania”) w rozsądnym stopniu zadowalającego dla Citi w celu monitorowania Skarg i zapewni Citi, według własnego uznania Citi, kopię raportów lub dostęp do systemu. System monitorowania będzie:
- kategoryzować Skargi według rodzaju, daty otrzymania oraz daty zgłoszenia Skargi do Citi;
 - śledzić przebieg rozpatrywania Skargi do czasu zakończenia/rozwiązania, a także
 - uwzględniać wszystkie inne kwestie, o które Citi może w uzasadniony sposób poprosić. System monitorowania musi być zaprojektowany w taki sposób, aby umożliwiać Dostawcy ustalenie, czy otrzymuje nadmierną liczbę Skarg dotyczących określonej kwestii, tak aby Dostawca (w porozumieniu z Citi) mógł ustalić, czy istnieje problem systemowy dotyczący działalności Dostawcy lub świadczenia przez niego Usług, i niezwłocznie rozwiązywać problemy.

21 POLITYKA DOTYCZĄCA TRANSAKCJI OSOBISTYCH I INWESTYCJI

Polityka Citi dotycząca transakcji osobistych i inwestycji (PTIP, Personal Trading and Investment Policy) określa dozwolone i zabronione działania handlowe i inwestycyjne, wymagania dotyczące wstępnej akceptacji oraz wymagania dotyczące prowadzenia, ujawniania i monitorowania rachunków maklerskich lub transakcyjnych Osób objętych regulacjami. Ustala minimalne standardy w celu promowania zgodności z przepisami i regulacjami, aby zapobiec niewłaściwemu wykorzystaniu pozycji osoby fizycznej lub jej relacji z Citi, w tym wiedzy tej osoby na temat (1) Istotnych informacji niepublicznych lub informacji wewnętrznych (łącznie zwanych „MNPI” [Material Non-Public Information]) dotyczących Citi lub strony trzeciej; lub (2) informacji dotyczących pozycji, transakcji i strategii klientów w zakresie papierów wartościowych, instrumentów pochodnych i towarów.

Cały personel Dostawcy, który wymaga regularnego dostępu do MNPI w ramach swoich obowiązków służbowych w Citi i jest wyznaczony jako Osoby objęte regulacjami i/lub

Osoby uzyskujące dostęp do Citi, musi przestrzegać wymogów w ramach PTIP. Pracownicy Dostawcy muszą stosować się do wniosków ICRM związanych z ujawnianiem danych o rachunkach osobistych, wstępnej akceptacji działań w zakresie transakcji osobistych i ograniczeń dotyczących transakcji osobistych oraz wymogu przekazywania okresowych zestawień.

22 STANDARDY ROZLICZEŃ I FAKTUROWANIA

W związku z wysiłkami Citi na rzecz poprawy terminowości usług i wzmocnienia mechanizmów kontroli wszyscy Dostawcy są zobowiązani do wspierania preferowanych przez Citi metod składania faktur, a także preferowanych opcji płatności za faktury, jak opisano poniżej:

- Dostawca utworzy pliki elektroniczne do przekazania Citi w formacie wskazanym Dostawcy przez Citi i/lub wykorzysta narzędzie Citi iSupplier do wprowadzenia wymaganych danych faktury/rozliczeniowych do późniejszego cyfrowego przekazania Citi.
- Dostawca dostarczy Citi wszystkie wymagane informacje bankowe i dokumentację uzupełniającą w celu ułatwienia realizacji płatności elektronicznych na rzecz Dostawcy i/lub korzystania z oferowanych przez Citi płatności kartą wirtualną (o ile jest to możliwe).

Uwaga: Warunki płatności są obliczane od daty otrzymania faktury przez Citi.

Aby zapewnić terminowe płatności i wypełnić zobowiązania umowne, Citi wymaga od wszystkich Dostawców podania następujących danych fakturowych i przestrzegania powiązanych wytycznych dotyczących fakturowania Citi za towary lub usługi:

1. Prawidłowa jednostka biznesowa Citi, adres rozliczeniowy i nazwa powiązanej osoby kontaktowej w Citi;
2. Numer faktury, data faktury i numer zlecenia zakupu;
3. Faktury należy przysyłać do lokalizacji Citi lub na adres e-mail podany w zleceniu zakupu Citi;
4. Towary i usługi podlegające rozliczeniu muszą być opisane na fakturze w sposób jasny i szczegółowy;
5. Należy uwzględnić wyłącznie bieżące opłaty dotyczące konkretnej faktury (nie należy uwzględniać innych niezapłaconych sald na fakturach);
6. Faktury, włącznie z dokumentacją uzupełniającą, muszą być sporządzane w języku angielskim.

23 POLITYKA OBOWIĄZKOWEJ NIEOBECNOŚCI

Polityka obowiązkowej nieobecności Citi wymaga od osób fizycznych, które prowadzą działania wrażliwe lub obarczone wysokim ryzykiem, zwłaszcza te mające wpływ na

księgi i zapisy firmy, okresowego odejścia od tych obowiązków. To wymuszone odsunięcie ma na celu wzmocnienie kontroli wewnętrznych poprzez stworzenie możliwości wykrywania potencjalnych nadużyć, kradzieży lub innych naruszeń, które w przeciwnym razie mogłyby pozostać ukryte. Polityka jest zgodna z oczekiwaniami nadzorczymi określonymi przez Zarząd Rezerw Federalnych Stanów Zjednoczonych w odniesieniu do wymaganych nieobecności personelu na stanowiskach o podwyższonym ryzyku.

Wszyscy pracownicy Dostawcy, którzy mają dostęp do danych poufnych i w ramach swoich obowiązków służbowych w Citi **oraz** którzy są określani jako osoby „pełniące funkcje wrażliwe”, muszą przestrzegać wymogów określonych w polityce MA. Osoby pełniące funkcje wrażliwe są zobowiązane co roku zaplanować i w pełni odbyć Obowiązkowy okres nieobecności, przestrzegając wszystkich zasad i ograniczeń określonych w polityce. W tym okresie nie wolno im wykonywać, zlecać, autoryzować ani zatwierdzać żadnych działań wrażliwych; nie powinni również udzielać merytorycznej odpowiedzi na żadną komunikację — włączając w to interakcje z klientami — za wyjątkiem przekierowania zapytań dotyczących zastępstwa. Jeśli okres nieobecności musi zostać przerwany po jego rozpoczęciu, kierownicy lub kontakty biznesowe Citi muszą anulować ten okres nieobecności w Systemach zgodności, aby dostęp do systemu został przywrócony, po czym Pracownik musi zaplanować nowy okres nieobecności.

ZAŁĄCZNIK — DEFINICJE

Szczelina powietrzna to rodzaj zabezpieczenia, w którym komputer, system lub sieć są fizycznie odizolowane od innych komputerów, systemów lub sieci. Architektura kopii zapasowych ze szczeliną powietrzną ogranicza ryzyko cyberataku i umożliwia przywrócenie danych do stanu przed rozpoczęciem ataku.

Obowiązujące prawo obejmuje: (a) stanowe przepisy i regulacje dotyczące egzekucji oraz (b) zasady, wytyczne i inne komunikaty wydawane przez różne agencje federalne Stanów Zjednoczonych, w tym Urząd Kontrolera Waluty (Office of the Controller of the Currency) (czasami określane jako wytyczne i przepisy dotyczące czerwonej flagi (Red Flag Guidelines), wdrażające sekcję 114 ustawy z 2003 r. o rzetelnym i dokładnym zapisie informacji o transakcjach kredytowych (Fair and Accurate Credit Transactions Act).

Strefa Dostępności to miejsce, w którym Dostawca usług w chmurze ma grupę logicznych centrów danych. Strefa dostępności to jedno centrum danych lub kilka centrów danych z nadmiarowym zasilaniem, siecią i telekomunikacją w Regionie chmury.

Sztuczna inteligencja (AI, Artificial Intelligence) odnosi się do ilościowej metody, systemu lub podejścia („technik”) naśladowujących ludzką inteligencję za pomocą programów komputerowych w celu tworzenia szacunków, prognoz, zaleceń lub podejmowania decyzji w sposób wykraczający poza klasyczne podejścia statystyczne, matematyczne, ekonometryczne lub finansowe. Obejmuje to wszystkie kategorie sztucznej inteligencji określone poniżej, a także warianty sztucznej inteligencji, na przykład: generatywną sztuczną inteligencję, Agentic AI, duże modele językowe, AI ogólnego przeznaczenia (GPAI) itp.

Kategorie sztucznej inteligencji obejmują:

- **Statyczna sztuczna inteligencja:** Techniki sztucznej inteligencji ręcznie szkolone w trybie offline lub których parametry są wyraźnie zaprogramowane, a następnie wykorzystywane do tworzenia szacunków, prognoz, zaleceń lub podejmowania decyzji.
- **Dynamiczna sztuczna inteligencja:** Techniki, które w przeciwieństwie do „Statycznej sztucznej inteligencji” mogą okresowo automatycznie przekwalifikowywać parametry; w produkcji.
- **Automatyczna sztuczna inteligencja:** techniki „Dynamicznej sztucznej inteligencji”, które dodatkowo umożliwiają automatyczną zmianę swojej podstawowej struktury (np. hiperparametry, zmienne wejściowe).
- **Kognitywna sztuczna inteligencja:** Techniki, które są zdolne do samodzielnego podejmowania decyzji i podejmowania odpowiednich działań, nawet w kwestiach, do których nie zostały specjalnie przeszkolone.

Uczenie maszynowe (Machine Learning, ML) to podzbiór sztucznej inteligencji, który tworzy reprezentacje lub wnioski z danych bez konieczności programowania każdego parametru lub kroku obliczeniowego, na przykład poprzez lasy losowe czy metody oparte na sieciach neuronowych. Techniki sztucznej inteligencji, które nie należą do podzbioru ML, obejmują natomiast m.in. logikę rozmytą, zaawansowane techniki parsowania zależności do przetwarzania języka naturalnego.

Właściciel działań biznesowych (BAO, Business Activity Owner) to pracownik Citi odpowiedzialny za wykonywanie określonych działań związanych z relacjami z Dostawcami i aktywne zarządzanie określonymi działaniami.

Pośrednik biznesowy to Dostawca zaangażowany przez Citi do działania w imieniu Citi w celu zidentyfikowania nowych możliwości biznesowych lub zarządzania istniejącymi relacjami z klientami.

Prezent biznesowy to przedmiot wartościowy (inny niż Spotkanie służbowe) wręczony pracownikowi Citi lub otrzymany przez niego w związku z działalnością Citi lub podmiotu zewnętrznego, zasadniczo z wyłączeniem przedmiotów o wartości nieprzekraczającej 25 USD.

Informacje Citi to informacje, które należą do Citi lub które firma Citi jest zobowiązana chronić podczas przechowywania, przetwarzania, przesyłania lub usuwania, zarówno w formie cyfrowej, jak i formach innych niż cyfrowa.

Klasyfikacja Informacji Citi obejmuje:

Informacje Poufne to Informacje o firmach i/lub podmiotach powiązanych z Citi, które nie dotyczą osób fizycznych i wymagają wysokiego poziomu ochrony. Naruszenie poufności, integralności lub dostępności tych informacji może mieć poważny wpływ na działalność, stan finansowy, franczyzobiorców lub klientów korporacyjnych Citi.

Informacje Poufne umożliwiające ustalenie tożsamości to Informacje osobowe dotyczące osoby fizycznej, które mogą ułatwić niezgodną z prawem działalność, taką jak kradzież tożsamości, oszustwo kredytowe lub inne oszustwo finansowe przeciwko tej osobie. Naruszenie poufności, integralności lub dostępności tych informacji może mieć istotny wpływ na daną osobę, między innymi na straty finansowe lub oszukanie.

- Elementy danych osobowych, które w połączeniu z innymi danymi osobowymi tworzą Informacje poufne PII, obejmują imię i nazwisko osoby lub dane kontaktowe (adres, numer telefonu lub adres e-mail) w połączeniu z następującymi danymi:
 - Elementy danych transakcji, które mogą umożliwić transfer środków lub mogą zostać wykorzystane do kradzieży tożsamości lub oszustwa, takie jak:
 - Numer karty kredytowej/debetowej
 - Kod weryfikacji karty (CVV) lub kod PIN
 - Dane z raportu kredytowego (wynik oceny zdolności kredytowej)
 - Pełna data urodzenia
 - Wydajność pracownika (pochwały / opinie zwrotne) lub informacje o wynagrodzeniach
 - Nagrania wideo, w tym z monitoringu i bankomatów
- Niektóre elementy danych osobowych powinny stanowić Poufne Informacje Umożliwiające Ustalenie Tożsamości:
 - Numer ubezpieczenia społecznego wydany przez rząd Stanów Zjednoczonych lub wydany przez rząd numer identyfikacyjny (który jest równoważny w użyciu i/lub zapewnia ochronę prawną na podobnym poziomie, co numer amerykańskiego ubezpieczenia społecznego), numer paszportu, numer prawa jazdy albo indywidualny numer identyfikacji podatkowej

Informacje wewnętrzne to Informacje, które nie dotyczą osoby fizycznej, są przeznaczone do celów biznesowych i wymagają umiarkowanego poziomu ochrony. Zakres poufności, integralności lub dostępności tych informacji może mieć **ograniczony wpływ** na zespół lub grupę roboczą.

- **Informacje umożliwiające ustalenie tożsamości (Personally Identifiable**

Information, PII) — Informacje osobowe to wszelkie informacje, które:

- umożliwiają identyfikację lub mogą zostać użyte do identyfikacji osoby lub gospodarstwa domowego (na przykład imię i nazwisko, podpis, adres, unikatowy identyfikator państwowy, taki jak numer ubezpieczenia społecznego lub numer rejestracyjny mieszkańca, data urodzenia, numer prawa jazdy);
- odnoszą się do, opisują lub mogą być powiązane z daną osobą lub gospodarstwem domowym albo mogą w sposób uzasadniony nawiązywać (bezpośrednio lub pośrednio) do danej osoby lub gospodarstwa domowego;
- mogą zostać użyte do uwierzytelnienia osoby fizycznej lub zapewnienia dostępu do jej konta (na przykład
- nazwa użytkownika, adres e-mail, hasło, PIN, numer identyfikacyjny, odpowiedzi na pytania zabezpieczające); lub odnoszą się do osoby fizycznej i mogą mieć charakter wrażliwy (na przykład osobiste informacje medyczne lub zdrowotne, numer konta, wartość konta).
- Do danych osobowych zalicza się również Chronione informacje zdrowotne (zgodnie z definicją amerykańskiej ustawy o przenoszeniu i odpowiedzialności za ubezpieczenia zdrowotne), Wrażliwe informacje osobiste oraz Informacje kredytowe (zgodnie z definicją zawartą w różnych przepisach dotyczących ochrony danych/prywatności oraz poufności bankowej).

Informacje publiczne to informacje dostępne bez ograniczeń dla osób spoza Citi lub przeznaczone do użytku publicznego, takie jak informacje prasowe o Citi lub artykuły na temat Citi publikowane w mediach.

Informacje zastrzeżone to Informacje ograniczone do wykorzystania przez konkretne osoby lub grupy. Informacje te są najbardziej wrażliwe dla firmy Citi lub jej podmiotów stowarzyszonych i wymagają najwyższego poziomu ochrony. Naruszenie poufności, integralności lub dostępności tych informacji może mieć **poważny wpływ (obejmujący całą firmę, wiele regionów, wiele sektorów)** na działalność, stan finansowy, franczyzobiorców lub klientów korporacyjnych Citi.

- **Wrażliwe Informacje Umożliwiające Ustalenie Tożsamości** to Informacje osobowe, które w świetle przepisów prawa wymagają dodatkowej ochrony, mogą zostać potencjalnie wykorzystane do niezgodnej z prawem dyskryminacji lub które w inny sposób mogą spowodować niesprawiedliwość lub szkodę dla danej osoby. Naruszenie poufności, integralności lub dostępności tych informacji może mieć istotny wpływ na daną osobę, między innymi na straty finansowe, dyskryminację lub oszukanie.
- Dane dotyczące w szczególności: rasy, religii, przekonań religijnych lub światopoglądu, narodowości, przynależności politycznej lub poglądów politycznych, członkostwa w związkach zawodowych, informacji dotyczących przeszłości kryminalnej lub przestępstw, danych genetycznych, danych biometrycznych lub danych dotyczących orientacji lub aktywności seksualnej danej osoby.
- Informacjami o stanie zdrowia, które obejmują informacje dotyczące historii choroby lub stanu psychicznego lub fizycznego danej osoby;

Klient oznacza każdego klienta Citi — mogą to być osoby (tj. osoby fizyczne) oraz przedsiębiorstwa, instytucje, organizacje bądź osoby prawne.

Region chmury to fizyczna lokalizacja, w której Dostawca usług w chmurze łączy centra danych w klastry.

Urządzenia, systemy i usługi komunikacyjne to wszelkie urządzenia, oprogramowanie lub aplikacje wykorzystywane do przesyłania elektronicznej korespondencji pisemnej, głosowej lub wideo. Kanały komunikacji elektronicznej obejmują między innymi: komputery, laptopy, tablety, urządzenia mobilne lub telefony komórkowe, w tym własne urządzenia do pracy (BYOD, Bring Your Own Device), BlackBerry, telefony, telefaksy (usługi faksowe), dostęp do intranetu i Internetu, usługi Wi-Fi, usługi poczty elektronicznej, usługi komunikacji błyskawicznej, takie jak Microsoft Lync, Skype i Bloomberg, witryny internetowe i aplikacje z wbudowanymi funkcjami komunikacji, platformy do spotkań wideo lub współpracy, takie jak Zoom lub Microsoft Teams, a także usługi mediów społecznościowych, interaktywne usługi udostępniania informacji, pokoje czatowe firm zewnętrznych, elektroniczne tablice ogłoszeń i blogi.

Treść oznacza Informacje poufne Citi oraz wszelkie inne dane, raporty, statystyki lub informacje dowolnego rodzaju (a) dostarczone lub udostępnione Dostawcy bezpośrednio lub pośrednio przez lub w imieniu Citi lub jej Podmiotów stowarzyszonych albo przez bądź w imieniu jego lub ich klientów lub usługodawców, (b) utworzone, wyprodukowane za pośrednictwem Usług lub (c) powstałe na podstawie któregośkolwiek z powyższych.

Umowa to dokument prawny podpisany przez co najmniej dwie strony, określający warunki oferty, akceptacji i wynagrodzenia, a także ustalający zobowiązania stron i zgodność celu z przepisami prawa. Przykłady Umów to: Umowa ramowa dotycząca produktów i usług, zakresy prac / zlecenia na wykonanie określonej pracy, zmiany i aneksy, harmonogramy, zlecenia i wszelkie inne dokumenty pisemne podpisane przez podmiot Citi i Dostawcę. Na potrzeby niniejszych Standardów Umowa o zachowaniu poufności (NDA, Non-Disclosure Agreement) również jest traktowana jak Umowa.

Test odmowy dostępu (DOA, Denial of Access) weryfikuje, czy Dostawca zapewnia odpowiednie obsadzenie personelem i wsparcie procesów biznesowych Citi, które mogą zostać przywrócone w ciągu wyznaczonego docelowego czasu przywrócenia działania.

Test odmowy usługi (DOS, Denial of Service) weryfikuje, czy aplikacja Dostawcy i podstawowe komponenty infrastruktury wspierające działalność Citi mogą zostać przywrócone w ciągu wyznaczonego docelowego czasu przywrócenia działania.

„Materiały depozytowe” oznaczają łącznie następujące podpunkty (i)–(vi), w odniesieniu do, w stosownych przypadkach, oprogramowania licencjonowanego dla Citi do użytku w środowisku Citi lub materiałów wykorzystywanych przez Dostawcę w ramach Usług hostowanych świadczonych na rzecz Citi:

- (i) Dokładna, zduplikowana wersja Kodu źródłowego oprogramowania wykorzystywanego do rozwoju, obsługi, konserwacji i wsparcia licencjonowanego oprogramowania lub Usług hostowanych określonych w odpowiedniej umowie z Citi (i wszystkich kolejnych wersjach takiego oprogramowania lub Usług hostowanych) oraz całej Dokumentacji dotyczącej takiego oprogramowania (niezależnie od tego, czy Citi posiada już kopię części takiego Kodu źródłowego) („**Depozyt kodu źródłowego**”);
- (ii) Kod źródłowy do jakiegokolwiek oprogramowania stron trzecich, do którego Dostawca ma prawa w odniesieniu do rozwijania, działania i konserwacji oraz wsparcia licencjonowanego oprogramowania lub Usług hostowanych;
- (iii) Licencjonowana kopia wszystkich narzędzi programowych, takich jak debugery, assemblyery i kompilatory, niezbędnych do konwersji Kodu źródłowego zawartego w Materiałach depozytowych do postaci wykonywalnej, w zakresie niezbędnym do obsługi, konserwacji i wspierania oprogramowania lub Usług hostowanych;
- (iv) W zakresie, w jakim nie zostało to jeszcze przedstawione powyżej, Dokumentacja zawiera: (A) ogólne opisy i sposób działania Materiałów depozytowych; (B) architekturę

- i podstawowe funkcje programu; (C) informacje o przepływie danych; (D) szczegółową mapę pamięci i listing; (E) mapy portów wejścia/wyjścia; oraz (F) inne szczegóły, które pozwoliłyby programistom o zwykłych umiejętnościach w odpowiednim języku programowania na użycie i modyfikację Kodu źródłowego zawartego w Materiałach depozytowych;
- (v) Wszystkie inne informacje techniczne związane z oprogramowaniem lub Usługami hostowanymi, jakie mogłyby być zasadnie wymagane w celu umożliwienia Citi lub właściwej stronie trzeciej w imieniu Citi korzystania, obsługi, modyfikowania i udoskonalania oprogramowania lub Usług hostowanych; oraz
 - (vi) Lista całego oprogramowania i wszystkich technologii stron trzecich używanych w związku z oprogramowaniem lub Usługami hostowanymi, w tym szczegółowe informacje dotyczące ich wykorzystania w oprogramowaniu oraz informacje kontaktowe dostawcy takiego oprogramowania lub technologii. Citi potwierdza i wyraża zgodę, że Materiały depozytowe nie zawierają żadnego kodu źródłowego od stron trzecich innych niż określone w podpunkcie (ii); oraz
 - (vii) w odniesieniu do Usług hostowanych:
 - a. pomniejszonej repliki środowiska produkcyjnego hostowanego w chmurze lub materiałów związanych z chmurą, specyficznych dla danego środowiska, oraz innych informacji wymaganych do odtworzenia środowiska produkcyjnego Citi, w tym (ale nie wyłącznie): infrastruktury jako kodu, skryptów Terraform, zasobów chmury, szablonów CloudFormation, plików konfiguracyjnych, klientów chmury, subskrypcji chmurowych, obrazów maszyn, obrazów Docker i infrastruktury jako kodu źródłowego oprogramowania; oraz
 - b. kopii danych Citi przechowywanych w oprogramowaniu.

Komunikacja elektroniczna to wiadomości lub informacje wysyłane, otrzymywane lub wykorzystywane przez Personel za pomocą środków elektronicznych, przesyłane przewodowo lub poprzez sygnały bezprzewodowe. Komunikacja elektroniczna obejmuje między innymi wiadomości tekstowe, wiadomości e-mail, wiadomości między użytkownikami (peer-to-peer) lub błyskawiczne, wpisy na blogach, wpisy w mediach społecznościowych, wiadomości wysyłane za pośrednictwem aplikacji do obsługi wiadomości, takich jak WhatsApp, WeChat, Line, Signal lub Viber, a także załączniki, zrzuty ekranu, nagrania głosowe lub pliki wideo, głos lub wideo na żywo, jak również pliki utworzone, otrzymane, pobrane, przechowywane, przesyłane, usuwane lub wykorzystywane za pośrednictwem urządzeń, systemów i usług komunikacji elektronicznej.

Identyfikatory funkcjonalne to identyfikatory ogólne, takie jak ADMIN lub ROOT, które są wykorzystywane przez osobę lub proces w celu uzyskania dostępu do systemu bezpieczeństwa. Kluczową inicjatywą w ramach operacji zarządzania tożsamością i dostępem (IAM) jest zapewnianie, że Citi ma wdrożone dedykowane, ściśle określone mechanizmy kontroli zapewniające ochronę przed zagrożeniami związanymi ze stosowaniem Identyfikatorów funkcjonalnych.

Procesy o znaczeniu krytycznym dla franczyzy / Aplikacje o znaczeniu krytycznym dla franczyzy (FCA) to procesy/aplikacje, które zostały wskazane przez Citi jako niezbędne do pomyślnego wykonywania funkcji biznesowych o znaczeniu krytycznym dla franczyzy.

Oszustwo jest celowym działaniem, błędnym oświadczeniem lub zaniechaniem, mającym na celu wprowadzenie w błąd innych osób. W wyniku oszustwa ofiara ponosi stratę albo sprawca osiąga korzyść.

Usługi hostowane obejmują wszelkie Zainstalowane aplikacje oraz wszelkie obiekty i środowiska zarządzane lub wykorzystywane przez Dostawcę w celu świadczenia Usług hostowanych, wszelkie aplikacje i inne oprogramowanie, bazy danych, witryny internetowe, serwery, sprzęt, sieci, sprzęt telekomunikacyjny i inny sprzęt oraz inną technologię zainstalowaną lub używaną w środowisku Usług hostowanych oraz, w każdym przypadku, wszystkie Aktualizacje i Usługi wsparcia, ale z wyłączeniem całej Treści i Systemów Citi.

Dane umożliwiające weryfikację tożsamości (IVD) zdefiniowane są jako pytania dotyczące bezpieczeństwa (SQ) lub pytania dotyczące uwierzytelniania opartego na wiedzy (KBA). Pytania dotyczące bezpieczeństwa są zwykle definiowane przez aplikację, a odpowiedzi na nie udziela użytkownik końcowy. Przykłady to nazwisko panieńskie matki, miejsce urodzenia, ulubione lody itp. Oba rodzaje pytań muszą być traktowane jako Dane uwierzytelniające.

Bezpieczeństwo informacji oznacza stan, w którym komputer lub system komputerowy są chronione przed nieuprawnionym dostępem lub atakiem, i ze względu na ten stan (a) komputer lub system komputerowy są nadal dostępne i funkcjonalne; (b) zachowana jest integralność komputera lub systemu komputerowego; oraz (c) zachowana jest integralność i poufność informacji przechowywanych i przetwarzanych na komputerze lub w systemie komputerowym lub przesyłanych za ich pośrednictwem.

Zagrożenie związane z bezpieczeństwem informacji oznacza czynność lub działanie (rozpoznane lub domniemane) wykonywane na komputerze lub w systemie komputerowym lub za pośrednictwem komputera lub systemu komputerowego, które to czynność lub działanie mogą zagrażać bezpieczeństwu informacji lub negatywnie na nie wpłynąć na tym lub innym komputerze lub systemie komputerowym.

Podatność w zakresie bezpieczeństwa informacji oznacza jakąkolwiek lukę w zabezpieczeniach komputera lub systemu komputerowego, która może zostać wykorzystana przez jedno lub więcej Zagrożeń związanych z bezpieczeństwem informacji.

Działania niezwiązane z obsługą klienta / niegenerujące przychodów są definiowane jako działania krytyczne dla działalności przedsiębiorstwa, niezwiązane z działaniami generującymi przychody, włączając w to działania prawne, nadzorcze, regulacyjne i związane z zapewnieniem ciągłości działania.

Umowa o zachowaniu poufności (NDA, Non-Disclosure Agreement) to umowa zawarta między Citi a Dostawcą, której postanowienia regulują wymianę, wykorzystywanie oraz ujawnianie Informacji.

Oprogramowanie typu open source to kod źródłowy lub skompilowany program komputerowy, którego kod źródłowy jest dostępny publicznie do użytku lub modyfikacji względem oryginalnego projektu.

Personel: oznacza, niezależnie od tego, czy zostało to określone bezpośrednio, czy wynika z kontekstu, Dostawcę i jego podmioty powiązane, dyrektorów, członków kadry kierowniczej, pracowników, przedstawicieli, audytorów, konsultantów, usługodawców i wykonawców (z wyłączeniem personelu Citi). Personel Dostawcy obejmuje również dyrektorów, urzędników, pracowników, przedstawicieli, audytorów, konsultantów i innych przedstawicieli dowolnego „Podwykonawcy”.

Rejestr dokumentów to szczegółowy wykaz uwzględniający rodzaj dokumentu, miejsce, datę itp. dokumentów Citi, który jest potrzebny jednostce biznesowej, aby mogła ona odpowiednio zarządzać swoimi dokumentami w trakcie Cyklu życia informacji.

Nakaz zachowania informacji to wymóg dotyczący Dokumentacji i Informacji, który zawiesza możliwość ich modyfikacji lub usuwania do czasu uchylecia przez organ, który wydał taki nakaz.

Zdolność odtworzeniowa to wolumen, ilość lub szybkość dostawy produktów i usług Dostawcy wyrażone jako odsetek normalnego poziomu dostawy produktów i usług.

Czas trwania przywracania to maksymalny okres liczony w dniach kalendarzowych, w którym Dostawca jest w stanie utrzymać operacje w trybie przywracania.

Docelowy punkt przywrócenia działania to określony punkt w czasie, wyrażony w godzinach, do którego należy przywrócić dane po nagłej przerwie w działalności. To maksymalny okres docelowy, w którym dane mogą zostać utracone z usług informatycznych w wyniku poważnego zdarzenia. Docelowy punkt przywrócenia działania to wyłącznie miara maksymalnego okresu, w którym dane mogą ulec utracie w przypadku poważnego zdarzenia mającego wpływ na usługi informatyczne. Nie jest to dokładna miara ilości danych, które mogą zostać utracone, na przykład do końca przetwarzania danych z poprzedniego dnia.

Docelowy czas przywrócenia działania to czas liczony w godzinach od chwili przerwania świadczenia usługi do momentu przywrócenia zapewniania produktów i usług.

„Zdarzenie wydania depozytu” oznacza co jedną z poniższych sytuacji lub więcej:

- (i) Dostawca (A) staje się niewypłacalny lub przyznaje, że nie jest w stanie spłacić swoich długów na ogół w miarę ich wymagalności; (B) staje się przedmiotem, dobrowolnie lub nieumyślnie, postępowania prowadzonego zgodnie z krajowym lub zagranicznym prawem upadłościowym, które nie zostało w pełni zatrzymane w ciągu siedmiu (7) dni roboczych lub nie zostało umorzone lub unieważnione w ciągu czterdziestu pięciu (45) dni po złożeniu wniosku; (C) dokonuje cesji ogólnej na rzecz wierzycieli; lub (D) ma syndyka, zarządcę komisyjnego, kuratora masy upadłościowej lub podobnego agenta wyznaczonego na mocy nakazu jakiegokolwiek sądu właściwej jurysdykcji do przejęcia lub sprzedaży jakiegokolwiek istotnej części swojego mienia lub firmy.

Organizacja zarządzania zasobami (RMO, Resource Management Organization) jest odpowiedzialna za globalne kompleksowe zarządzanie zasobami w Citi, w tym zaopatrzenie strategiczne, operacje od zakupu do zapłaty, biuro kadr i ramy zarządzania dostawcami.

RMO Sourcing Manager to osoba fizyczna w Organizacji zarządzania zasobami (RMO), która jest odpowiedzialna za negocjowanie warunków handlowych, cenowych i wymogów Umowy, w tym

RFP i innych czynności związanych z dokonaniem wyboru Dostawcy, a także za postępowanie zgodnie z warunkami Umowy oraz wymogami dotyczącymi akredytacji oceny finansowej.

Poważny lub katastrofalny wpływ na daną osobę to wpływ, który w uzasadniony sposób może prowadzić do istotnych skutków niepożądanych dla danej osoby, w tym straty finansowej, utraty zatrudnienia, utraty lub trudności w znalezieniu zatrudnienia, utraty praw człowieka, osobistego lub publicznego upokorzenia lub niesłusznego pozbawienia wolności.

Podwykonawca: Podwykonawca to czwarta strona (osoba lub podmiot), która została zatrudniona przez stronę trzecią do wykonywania niektórych lub wszystkich usług albo działań zakontraktowanych przez Citi stronie trzeciej.

Wskazówki:

P1: Czy wszyscy podwykonawcy Strony trzeciej muszą być zgłaszani?

O1: Należy zgłaszać wyłącznie podwykonawców związanych z wykonywaną usługą. Poniżej przedstawiono przykładowe usługi lub działania realizowane przez podwykonawcę:

*Podwykonawca świadczący usługi technologiczne lub programowe, bezpośrednio lub pośrednio wspierające usługę/działania, które Citi zakontraktowało ze Stroną trzecią; lub

*Podwykonawca, którego usługi wymagają dostępu do informacji sklasyfikowanych przez Citi jako Poufne lub o wyższej klauzuli tajności; lub

*Podwykonawca, który nawiązuje bezpośrednią lub pośrednią interakcję z istniejącym/potencjalnym Klientem Citi; lub

*Podwykonawca, który nie jest eskortowany i odpowiada za niszczenie lub archiwizację dokumentów Citi w ramach jakiegokolwiek siedziby Citi lub poza nią; lub

*Podwykonawca wspierający podstawowe funkcje lub usługi bankowe, takie jak płatności, windykacja, udzielanie pożyczek itp.

Dostawca: Do celów niniejszego dokumentu „Wymagania Citi dla Dostawców” termin „Dostawca” odnosi się wyłącznie do Zewnętrznej strony trzeciej, która zawarła umowę biznesową w celu dostarczania produktów lub usług bezpośrednio Podmiotowi Citi lub wspierania Podmiotu Citi w realizacji jego celów biznesowych. Zewnętrzna strona trzecia jest zdefiniowana jako podmiot inny niż Citi. Dostawcy mogą również być klientami Podmiotu Citi lub mogą wspierać interakcje z klientami Citi; jednak ustalenia oparte wyłącznie na fakcie bycia klientem Citi nie są uważane za relacje z dostawcami w rozumieniu niniejszego dokumentu.

Informacje przejściowe: Dokument to ostateczna, najbardziej kompletna wersja informacji, które Citi ma obowiązek zachować z powodów prawnych, regulacyjnych lub zatwierdzonych powodów biznesowych. Wszystkie inne informacje są klasyfikowane jako „Informacje przejściowe”.