Warunki Używania Produktów i Usług IBM — Warunki Specyficzne dla Oferty Usług SaaS

IBM Security Trusteer Fraud Protection

Warunki Używania (zwane dalej „Warunkami Używania”) składają się z niniejszych „Warunków Używania Produktów i Usług IBM — Warunków Specyficznych dla Oferty Usług SaaS” (zwanych dalej „Warunkami Specyficznymi dla Oferty Usług SaaS”) oraz dokumentu pt. „Warunki Używania Produktów i Usług IBM — Warunki Ogólne” (zwanego dalej „Warunkami Ogólnymi”) dostępnego pod adresem: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

W przypadku sprzeczności Warunki Specyficzne dla Oferty Usług SaaS mają znaczenie rozstrzygające nad Warunkami Ogólnymi. Zamawiając usługę IBM SaaS, uzyskując do niej dostęp lub korzystając z niej, Klient wyraża zgodę na niniejsze Warunki Używania.

Niniejsze Warunki Używania podlegają Międzynarodowej Umowie IBM Passport Advantage, Międzynarodowej Umowie IBM Passport Advantage Express lub Międzynarodowej Umowie IBM Dotyczącej Wybranych Ofert Usług IBM SaaS (zwanej dalej „Umową”), która razem z Warunkami Używania stanowi całość umowy.

1. Usługi IBM SaaS

Niniejsze Warunki Specyficzne dla Oferty Usług SaaS dotyczą następujących usług IBM SaaS:

1.1 Oferty usług Rapport IBM SaaS

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Oferty usług Pinpoint IBM SaaS

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support

- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Oferty usług IBM SaaS dla urządzeń mobilnych

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Opłaty rozliczeniowe

Przy sprzedaży usługi IBM SaaS wysokość opłat rozliczeniowych jest ustalana na podstawie następującej miary określonej w Dokumencie Transakcyjnym:

a. Jednostką miary, według której można korzystać z usługi IBM SaaS, jest **Uprawniony Uczestnik**. Uprawnionym Uczestnikiem jest każda osoba oraz każdy podmiot uprawniony do uczestnictwa w dowolnym programie świadczenia usługi zarządzanym lub monitorowanym za pomocą usługi IBM SaaS. Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę wszystkich Uprawnionych Uczestników objętych zarządzaniem lub śledzeniem w ramach usługi IBM SaaS w okresie pomiarowym określonym w Dokumencie Transakcyjnym.

   Każdy program świadczenia usług zarządzany za pomocą usługi SaaS podlega odrębnej analizie, a następnie jest rozpatrywany łącznie z pozostałymi programami. Osoby fizyczne lub jednostki zakwalifikowane do wielu programów świadczenia usług muszą uzyskać odrębne uprawnienia.

   W przypadku niniejszych ofert program świadczenia usług obejmuje pojedynczą Aplikację Biznesową lub Aplikację Indywidualną Klienta oraz główną stronę logowania i powiązane strony każdej Aplikacji Biznesowej lub Aplikacji Indywidualnej. Uprawniony Uczestnik to użytkownik końcowy w firmie Klienta, który posiada dane uwierzytelniające umożliwiające zalogowanie się w Aplikacji Biznesowej lub Indywidualnej.

b. Jednostką miary, według której można korzystać z usług IBM SaaS, jest **Urządzenie Klienckie**. Urządzenie Klienckie to pojedyncze urządzenie komputerowe lub telemetryczne bądź pojedyncze urządzenie w postaci czujnika specjalnego przeznaczenia, które żąda wykonania lub otrzymuje do wykonania zestaw komend, procedur lub aplikacji z innego systemu komputerowego bądź też dostarcza dane do takiego systemu, zazwyczaj określanego jako serwer lub zarządzanego w inny sposób przez serwer. Wiele Urządzeń Klienckich może współużytkować dostęp do jednego serwera. Aby umożliwić użytkownikowi wykonywanie pracy, Urządzenie Klienckie może być programowalne lub wyposażone w funkcje przetwarzania. Klient musi uzyskać uprawnienia dla każdego Urządzenia Klienckiego, które uruchamia usługę IBM SaaS, dostarcza do niej dane, korzysta z udostępnianych przez nią usług lub w inny sposób uzyskuje do niej dostęp w okresie pomiarowym wyszczególnionym w Dokumencie Transakcyjnym Klienta.

3. Opłaty i rozliczenia

Kwota należna do zapłaty za usługę IBM SaaS jest określona w Dokumencie Transakcyjnym.

3.1 Opłaty za niepełne miesiące

Opłata za niepełny miesiąc, zgodnie z treścią Dokumentu Transakcyjnego, może być naliczana w ujęciu proporcjonalnym.

4. Zachowanie zgodności i kontrola

Dostęp do ofert IBM Security Trusteer Fraud Protection jest ograniczony maksymalną liczbą Uprawnionych Uczestników lub Urządzeń Klienckich, zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym. Klient zobowiązuje się dopilnować, aby liczba Uprawnionych Uczestników lub Urządzeń Klienckich nie przekraczała wartości maksymalnej określonej w Dokumencie Transakcyjnym.

W celu sprawdzenia zgodności z maksymalną liczbą Uprawnionych Uczestników lub Urządzeń Klienckich może zostać przeprowadzona kontrola.

5. Możliwości odnowienia Okresu Subskrypcji usługi IBM SaaS

W Dokumencie Transakcyjnym Klienta zostanie wskazane, czy usługa IBM SaaS będzie odnawiana z końcem Okresu Subskrypcji. Poniżej opisano dostępne opcje.

5.1 Automatyczne odnowienie

Jeśli w Dokumencie Transakcyjnym Klienta wskazano, że odnowienie następuje automatycznie, Klient może zrezygnować z usługi IBM SaaS przed końcem dotychczasowego okresu subskrypcji przez złożenie pisemnego wypowiedzenia przedstawicielowi handlowemu IBM lub Partnerowi Handlowemu IBM nie później niż na 90 (dziewięćdziesiąt) dni przed datą wygaśnięcia okresu subskrypcji wskazaną w Dokumencie Transakcyjnym. Jeśli IBM ani Partner Handlowy IBM nie otrzyma wypowiedzenia przed upływem terminu wygaśnięcia, wygasający Okres Subskrypcji zostanie automatycznie przedłużony na kolejny rok lub inny okres równy pierwotnemu Okresowi Subskrypcji określonemu w Dokumencie Transakcyjnym.

5.2 Rozliczanie ciągłe

Jeśli w Dokumencie Transakcyjnym wskazano, że w przypadku Klienta obowiązuje ciągły tryb odnawiania, to Klient zachowa dostęp do usługi IBM SaaS, a korzystanie z niej będzie rozliczane w sposób ciągły. Aby zakończyć korzystanie z usługi IBM SaaS i proces rozliczania ciągłego, Klient będzie musiał przedstawić IBM lub Partnerowi Handlowemu IBM pismo z wnioskiem o anulowanie usługi IBM SaaS z wyprzedzeniem 90 (dziewięćdziesięciu) dni. Po anulowaniu dostępu Klienta do usługi Klient otrzyma fakturę z tytułu wszelkich nierozliczonych opłat za dostęp w miesiącu, w którym weszło w życie anulowanie.

5.3 Wymagane odnowienie

Jeśli w Dokumencie Transakcyjnym wskazano, że w przypadku Klienta obowiązuje typ odnowienia „rozwiązanie”, to w momencie zakończenia Okresu Subskrypcji świadczenie usługi IBM SaaS zostanie zakończone, a Klient utraci dostęp do niej. Aby móc nadal korzystać z usługi IBM SaaS po upływie terminu zakończenia, Klient będzie musiał złożyć u przedstawiciela handlowego lub Partnera Handlowego IBM zamówienie na zakup nowego Okresu Subskrypcji.

6. Wsparcie Techniczne

Klientowi i Uprawnionym Uczestnikom udostępniane jest wsparcie techniczne do usługi IBM SaaS, aby pomagać im w korzystaniu z tej usługi.

Wsparcie Standardowe jest uwzględnione w subskrypcji każdej oferty. W przypadku usługi Trusteer Rapport Mandatory Service, stanowiącej dodatek do usługi Trusteer Rapport, wymaganiem wstępnym jest posiadanie Wsparcia Premium w odniesieniu do podstawowej subskrypcji usługi Trusteer Rapport.

W przypadku każdej oferty IBM SaaS subskrypcja Wsparcia Premium jest dostępna za dodatkową opłatą. Wyjątek stanowią oferty IBM Security Trusteer Mobile SDK oraz IBM Security Trusteer Rapport Mandatory Service.

Wsparcie standardowe:

- Wsparcie jest świadczone w godzinach od 8:00 do 17:00 czasu miejscowego.
- Klienci i Uprawnieni Uczestnicy mogą wprowadzać zgłoszenia problemów w postaci elektronicznej zgodnie ze szczegółowym opisem w Podręczniku Wsparcia SaaS.
- Klienci mogą uzyskać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem http://www-01.ibm.com/software/security/trusteer/support/.
- Wykaz opcji wsparcia oraz inne szczegółowe informacje na temat wsparcia można znaleźć w Podręczniku Wsparcia SaaS pod adresem http://www-01.ibm.com/software/support/handbook.html.

Wsparcie Premium:

- Wsparcie jest świadczone przez całą dobę we wszystkie dni tygodnia bez względu na poziom istotności.
- Klienci mogą uzyskać bezpośredni telefoniczny dostęp do wsparcia.
- Klienci i Uprawnieni Uczestnicy mogą wprowadzać zgłoszenia problemów w postaci elektronicznej zgodnie ze szczegółowym opisem w Podręczniku Wsparcia SaaS.
- Klienci mogą uzyskać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem http://www-01.ibm.com/software/security/trusteer/support/.
- Wykaz opcji wsparcia oraz inne szczegółowe informacje na temat wsparcia można znaleźć w Podręczniku Wsparcia SaaS pod adresem http://www-01.ibm.com/software/support/handbook.html.

7. Warunki dodatkowe dla oferty usług IBM SaaS

7.1 Zgodność z programem Safe Harbor

IBM przestrzega zasad programu U.S.–EU Safe Harbor Framework, opracowanego przez Departament Handlu Stanów Zjednoczonych w porozumieniu z Komisją Europejską. Produkty IBM Security Trusteer są objęte zakresem certyfikatu EU–U.S. Safe Harbor uzyskanego przez IBM. Więcej informacji na temat programu Safe Harbor oraz listę przedsiębiorstw, które go realizują, można znaleźć na stronie http://export.gov/safeharbor/.

7.2 Coroczna podwyżka Opłaty za Subskrypcję

IBM zastrzega sobie prawo do korygowania opłaty za subskrypcję usługi IBM SaaS nie częściej niż raz na dwanaście (12) miesięcy. Wysokość podwyżki będzie ustalana przez IBM, przy czym nie może ona przekroczyć 3%. Korekta opłaty za subskrypcję obowiązuje od rocznicy rozpoczęcia początkowego okresu obowiązywania. Korekta opłat nie wpływa na uprawnienia Klienta dotyczące usługi IBM SaaS ani na jednostkę miary służącą do obliczania opłat rozliczeniowych, według której można korzystać z usługi IBM SaaS. Partnerzy Handlowi IBM są niezależni od IBM i jednostronnie ustalają swoje ceny i warunki.

7.3 Wsparcie Premium

Klient ma uprawnienia do Wsparcia Premium wyłącznie w odniesieniu do tych ofert usług IBM SaaS, w odniesieniu do których Klient dokonał subskrypcji powiązanej oferty Wsparcia Premium.

7.4 Legalne używanie i wyrażenie zgody

Zgoda na gromadzenie i przetwarzanie danych

Usługa IBM SaaS została zaprojektowana z myślą o ułatwieniu Klientowi wprowadzania usprawnień dotyczących środowiska zabezpieczeń i przetwarzania danych. Usługa IBM SaaS będzie gromadzić informacje pochodzące od Uprawnionych Uczestników i Urządzeń Klienckich komunikujących się z Aplikacjami Biznesowymi lub Aplikacjami Indywidualnymi, które są objęte ofertami usług IBM SaaS zasubskrybowanymi przez Klienta. Usługa IBM SaaS gromadzi informacje, które same w sobie lub w określonym połączeniu mogą być uznane za Dane Osobowe według ustawodawstwa niektórych krajów. Dane Osobowe oznaczają wszelkie informacje, które mogą posłużyć do zidentyfikowania konkretnej osoby (takie jak imię i nazwisko, adres e-mail, adres zamieszkania lub numer telefonu), udostępniane IBM w celu przechowywania, przetwarzania lub przekazywania w imieniu Klienta.

Procedury gromadzenia i przetwarzania danych mogą być aktualizowane w celu poprawienia funkcjonalności usługi IBM SaaS. Dokument z pełnym opisem procedur gromadzenia i przetwarzania danych podlega aktualizacji zależnie od potrzeb i jest udostępniany Klientowi na żądanie. Klient

upoważnia IBM do gromadzenia powyższych informacji oraz ich przetwarzania zgodnie z postanowieniami paragrafów „Przekazywanie danych za granicę” i „Ochrona danych” niniejszych Warunków Używania, a także paragrafu Warunków Ogólnych zatytułowanego „Ochrona i bezpieczeństwo danych”.

W przypadku ofert IBM Security Trusteer Pinpoint:

Zgromadzone dane mogą obejmować adres IP użytkownika, ID użytkownika w postaci zaszyfrowanej lub przetworzonej przez jednokierunkową funkcję mieszającą, informacje cookie z domeny (o ile nie zostały odfiltrowane), informacje o położeniu geograficznym, informacje o odwiedzaniu aplikacji chronionych i serwisów służących do wyłudzania informacji oraz dane uwierzytelniające wpisane w takich serwisach.

W przypadku ofert IBM Security Trusteer Mobile SDK oraz IBM Security Trusteer Mobile Browser:

Zgromadzone dane mogą obejmować adres IP użytkownika, ID użytkownika w postaci zaszyfrowanej lub przetworzonej przez jednokierunkową funkcję mieszającą, lokalizację geograficzną, informacje o odwiedzaniu aplikacji chronionych, informacje o karcie SIM, nazwę urządzenia oraz informacje o przynależności organizacyjnej Klienta.

W przypadku ofert IBM Security Trusteer Rapport:

Zgromadzone dane mogą obejmować adres IP użytkownika, ID użytkownika w postaci zaszyfrowanej lub przetworzonej przez jednokierunkową funkcję mieszającą, informacje o zdarzeniach związanych z bezpieczeństwem, nazwę i adres e-mail użytkownika przekazane na potrzeby kontaktowania się z IBM w celu uzyskania wsparcia, przynależność organizacyjną Klienta, zaszyfrowane hasło wpisywane w chronionych serwisach, informacje o odwiedzaniu aplikacji chronionych i serwisów służących do wyłudzania informacji, zaszyfrowany numer karty płatniczej oraz pliki i dane zgromadzone zdalnie przez personel IBM w celu badania potencjalnie szkodliwego oprogramowania, szkodliwych działań lub wadliwego działania.

Świadoma zgoda właścicieli danych:

Korzystanie z niniejszej usługi IBM SaaS może podlegać różnym przepisom i regulacjom. Z usługi IBM SaaS można korzystać wyłącznie do celów zgodnych z prawem oraz w sposób zgodny z prawem. Klient zobowiązuje się korzystać z usługi IBM SaaS w sposób zgodny z odpowiednimi przepisami, regulacjami i strategiami oraz przyjmuje pełną odpowiedzialność za przestrzeganie takich przepisów, regulacji i strategii.

W przypadku ofert IBM Security Trusteer Pinpoint oraz IBM Security Trusteer Mobile SDK:

Klient potwierdza, że uzyskał lub uzyska wszelkie w pełni świadome zgody, uprawnienia lub licencje, które są niezbędne, aby umożliwić zgodne z prawem korzystanie z usługi IBM SaaS oraz aby zezwolić IBM na gromadzenie i przetwarzanie informacji za pośrednictwem usługi IBM SaaS.

W przypadku ofert IBM Security Trusteer Rapport oraz IBM Security Trusteer Mobile Browser:

Klient upoważnia IBM do uzyskania w pełni świadomej zgody, która jest niezbędna, aby umożliwić zgodne z prawem korzystanie z usługi IBM SaaS oraz aby gromadzić i przetwarzać informacje na zasadach opisanych w Umowie Licencyjnej z Użytkownikiem Końcowym dostępnej pod adresemhttps://www.trusteer.com/support/end-user-license-agreement. Jeśli Klient ustalił, że to Klient (a nie IBM) będzie kontaktować się z użytkownikami końcowymi w celu uzyskania ich zgody, wówczas Klient potwierdza, że uzyskał lub uzyska wszelkie w pełni świadome zgody, uprawnienia lub licencje, które są niezbędne, aby umożliwić zgodne z prawem korzystanie z usługi IBM SaaS oraz aby zezwolić IBM — jako podmiotowi przetwarzającemu dane na rzecz Klienta — na gromadzenie i przetwarzanie informacji za pośrednictwem usługi IBM SaaS.

7.5 Przekazywanie danych za granicę

Klient wyraża zgodę na przetwarzanie przez IBM zawartości (w tym wszelkich Danych Osobowych) poza granicami kraju w sposób zgodny z odpowiednimi przepisami i wymaganiami za pośrednictwem podmiotów przetwarzających i podwykonawców przetwarzania w następujących krajach spoza Europejskiej Strefy Ekonomicznej oraz w krajach, które zdaniem Komisji Europejskiej zapewniają należyty poziom bezpieczeństwa: Stany Zjednoczone.

7.6 Ochrona danych

Jeśli Klient udostępnia Dane Osobowe w ramach usługi IBM SaaS w krajach członkowskich Unii Europejskiej, w Islandii, Liechtensteinie, Norwegii lub Szwajcarii lub jeśli w krajach tych znajdują się Uprawnieni Uczestnicy bądź Urządzenia Klienckie z firmy Klienta, wówczas Klient, jako wyłączny administrator, mianuje IBM podmiotem przetwarzającym Dane Osobowe (zgodnie z definicją tych terminów w dyrektywie 95/46/WE). IBM będzie przetwarzać takie Dane Osobowe tylko w zakresie wymaganym do udostępnienia usługi IBM SaaS zgodnie z opublikowanymi przez IBM opisami usługi IBM SaaS, a Klient potwierdza, że przetwarzanie to jest zawsze zgodne z jego instrukcjami. IBM poinformuje Klienta z należytym wyprzedzeniem w przypadku wprowadzenia istotnych zmian w lokalizacji przetwarzania lub metodach ochrony Danych Osobowych przetwarzanych w ramach usługi IBM SaaS. Klient może zakończyć bieżący Okres Subskrypcji usługi IBM SaaS objętej taką zmianą, przekazując IBM pisemne wypowiedzenie w terminie 30 (trzydziestu) dni od otrzymania od IBM powiadomienia o zmianie. Klient wyraża zgodę na przetwarzanie przez IBM zawartości (w tym wszelkich Danych Osobowych) poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja*
Jednostka zlecająca IBM	Podmiot przetwarzający	Zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services LLC	Podwykonawca przetwarzania	410 Terry Ave. N Seattle, WA 98109 Stany Zjednoczone
Connectria Corp.	Podwykonawca przetwarzania	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Stany Zjednoczone
IBM Israel Ltd.	Podwykonawca przetwarzania	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael
IBM Corp	Podwykonawca przetwarzania	1 New Orchard Rd. Armonk, NY 10504 Stany Zjednoczone

Klient uznaje również, że IBM może zmieniać powyższą listę państw (pod warunkiem przekazania stosownego powiadomienia), jeśli uzna (mając ku temu podstawy), iż jest to konieczne do świadczenia usługi IBM SaaS.

W odniesieniu do usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech (co zostanie wskazane podczas udostępniania usługi), Klient wyraża zgodę na przetwarzanie przez IBM zawartości, w tym wszelkich Danych Osobowych, poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja*
Jednostka zlecająca IBM	Podmiot przetwarzający	Zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services (Niemcy)	Podwykonawca przetwarzania	Monachium, Niemcy
IBM Israel Ltd.	Podwykonawca przetwarzania	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

W odniesieniu do usług świadczonych za pośrednictwem centrum przetwarzania danych w Japonii (co zostanie wskazane podczas udostępniania usługi), Klient wyraża zgodę na przetwarzanie przez IBM zawartości, w tym wszelkich Danych Osobowych, poza granicami kraju za pośrednictwem następujących podmiotów przetwarzających i podwykonawców przetwarzania:

Nazwa podmiotu przetwarzającego/podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja*
Jednostka zlecająca IBM	Podmiot przetwarzający	Zgodnie z wyszczególnieniem w Dokumencie Transakcyjnym
Amazon Web Services (Japonia)	Podwykonawca przetwarzania	Tokio, Japonia
IBM Israel Ltd.	Podwykonawca przetwarzania	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

* Lokalizacje wyszczególnione w powyższych tabelach wskazują adresy siedziby podmiotu przetwarzającego / podwykonawcy przetwarzania. Centra przetwarzania danych są zlokalizowane w podanym kraju.

Strony lub ich odpowiednie przedsiębiorstwa afiliowane mogą zawrzeć oddzielne umowy sporządzone na podstawie standardowych, niezmodyfikowanych dokumentów wzorcowych UE (stosownie do ról poszczególnych podmiotów) zgodnie z Decyzją KE nr 2010/87/UE, z pominięciem klauzul opcjonalnych. Wszelkie spory i zobowiązania wynikające z powyższych umów (nawet jeśli umowy te zostaną zawarte przez przedsiębiorstwa afiliowane) będą traktowane jako spory i zobowiązania powstałe między Stronami zgodnie z warunkami niniejszej Umowy.

Dodatek A

1. Oferty usług IBM SaaS

IBM oferuje omawiane usługi jako usługi i oferty autonomiczne lub jako usługi i oferty dodatkowe. Konkretne oferty usług IBM SaaS zamówione przez Klienta zostały wyszczególnione w dokumencie PoE.

1.1 Definicje Aplikacji Biznesowej i Aplikacji Indywidualnej

Produkty IBM Security Trusteer do ochrony przed oszustwami są objęte licencją na używanie w powiązaniu z konkretnymi rodzajami Aplikacji. Zdefiniowane zostały dwa rodzaje Aplikacji: Aplikacja Indywidualna oraz Aplikacja Biznesowa. Dla każdego z tych rodzajów Aplikacji dostępne są odrębne oferty.

- Aplikacja Indywidualna oznacza aplikację bankowości elektronicznej, aplikację dla urządzeń mobilnych lub aplikację do handlu elektronicznego zaprojektowaną z myślą o obsłudze konsumenta. Zgodnie ze strategią obsługi Klienta niektórym małym przedsiębiorstwom może przysługiwać dostęp do oferty indywidualnej.
- Aplikacja Biznesowa oznacza aplikację bankowości elektronicznej, aplikację dla urządzeń mobilnych lub aplikację do handlu elektronicznego zaprojektowaną z myślą o obsłudze przedsiębiorstw, instytucji i podmiotów o równoważnej kategorii, a także dowolną aplikację, która nie została sklasyfikowana jako Aplikacja Indywidualna.

1.2 Oferty podstawowej subskrypcji usług IBM SaaS

Oferty biznesowe:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Oferty indywidualne:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

W przypadku każdej oferty biznesowej i indywidualnej dostępne jest powiązane Wsparcie Premium za dodatkową opłatą. Wyjątek stanowią oferty IBM Security Trusteer Mobile SDK.

1.3 Dodatkowe oferty subskrypcji usług IBM SaaS dotyczące ofert IBM Security Trusteer Rapport

Dodatkowe oferty dostępne w odniesieniu do usługi IBM Security Trusteer Rapport for Business:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Dodatkowe oferty dostępne w odniesieniu do usługi IBM Security Trusteer Rapport for Retail:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

W przypadku każdego biznesowego lub indywidualnego programu dodatkowego do ofert IBM Security Trusteer Rapport dostępne jest powiązane Wsparcie Premium za dodatkową opłatą. Wyjątek stanowią programy dodatkowe IBM Security Trusteer Rapport Mandatory Service.

W przypadku dodatkowych powiązanych ofert subskrypcji IBM SaaS wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji usług IBM Security Trusteer Rapport for Business lub IBM Security Trusteer Rapport for Retail.

1.4 Dodatkowe oferty subskrypcji usług IBM SaaS dotyczące ofert IBM Security Trusteer Pinpoint Malware Detection

Dodatkowe oferty dostępne w odniesieniu do usług IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition lub IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Dodatkowe oferty dostępne w odniesieniu do usług IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition lub IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

W przypadku każdej dodatkowej oferty IBM SaaS wymienionej w niniejszym paragrafie dostępna jest subskrypcja Wsparcia Premium za dodatkową opłatą.

W przypadku dodatkowych powiązanych ofert subskrypcji IBM SaaS wymienionych w niniejszym paragrafie wymaganiem wstępnym jest posiadanie subskrypcji ofert IBM Security Trusteer Pinpoint Malware Detection for Business lub IBM Security Trusteer Pinpoint Malware Detection for Retail.

1.5 Pozostałe dodatkowe subskrypcje usług IBM SaaS

Wszelkie dodatkowe subskrypcje usług IBM SaaS, które dotyczą wymienionych powyżej subskrypcji podstawowych, lecz nie zostały wymienione w niniejszym dokumencie, nie stanowią aktualizacji i muszą zostać nabyte oddzielnie (bez względu na to, czy są obecnie dostępne, czy też znajdują się na etapie opracowywania).

1.6 Definicje

Posiadacz Konta — użytkownik końcowy z firmy Klienta, który zainstalował klienckie oprogramowanie pomocnicze, zaakceptował Umowę Licencyjną z Użytkownikiem Końcowym oraz przynajmniej raz uwierzytelnił się w posiadanej przez Klienta Aplikacji Indywidualnej lub Biznesowej, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS.

Oprogramowanie Klienckie Posiadacza Konta — klienckie oprogramowanie pomocnicze IBM Security Trusteer Rapport, klienckie oprogramowanie pomocnicze IBM Security Trusteer Mobile Browser lub dowolne inne klienckie oprogramowanie pomocnicze dostarczane w ramach subskrypcji niektórych usług IBM SaaS i przeznaczone do zainstalowania na urządzeniu użytkownika końcowego.

Ekran powitalny Trusteer — ekran powitalny dostarczany Klientowi zależnie od dostępnych szablonów.

Strona Docelowa — strona udostępniana Klientowi przez IBM wraz ekranem powitalnym Klienta oraz Oprogramowaniem Klienckim Posiadacza Konta do pobrania.

2. Oferty IBM Security Trusteer Rapport

2.1 Oferta IBM Security Trusteer Rapport for Retail i/lub IBM Security Trusteer Rapport for Business („Trusteer Rapport”)

Oferta Trusteer Rapport zapewnia warstwę ochrony przed wyłudzaniem informacji i przed szkodliwym oprogramowaniem typu MitB (ang. Man in the Browser). Usługa ta wykorzystuje sieć kilkudziesięciu milionów punktów końcowych rozmieszczonych na wszystkich kontynentach, aby gromadzić dane analityczne o aktywnych atakach skierowanych przeciwko organizacjom z całego świata, a polegających

na wyłudzaniu informacji lub posługiwaniu się szkodliwym oprogramowaniem. W usłudze IBM Security Trusteer Rapport zastosowano algorytmy analizy zachowania, których celem jest blokowanie ataków związanych z wyłudzaniem informacji oraz zapobieganie instalowaniu i działaniu poszczególnych odmian szkodliwego oprogramowania typu MitB.

Jednostką miary, według której nalicza się opłaty za niniejszą ofertę usług IBM SaaS, jest Uprawniony Uczestnik. W przypadku oferty biznesowej sprzedawane są pakiety obejmujące dziesięciu Uprawnionych Uczestników, a w przypadku oferty indywidualnej — stu Uprawnionych Uczestników.

Niniejsza oferta usług IBM SaaS zawiera:

a. Aplikację Trusteer Management Application („TMA”):

   Aplikacja TMA jest udostępniana w środowisku IBM Security Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może: (i) otrzymywać raporty z danymi o zdarzeniach i oceny ryzyka, (ii) wyświetlać, konfigurować i ustalać strategie związane z raportowaniem danych o zdarzeniach, a także (iii) wyświetlać konfigurację klienckiego oprogramowania pomocniczego, które podlega bezpłatnej publicznej licencji na warunkach Umowy Licencyjnej z Użytkownikiem Końcowym, jest udostępnione do pobrania na komputery desktop i inne urządzenia (komputery PC/MAC) Uprawnionych Uczestników i jest znane również pod nazwą pakiet oprogramowania Trusteer Rapport („Oprogramowanie Klienckie Posiadacza Konta”). Klient może prowadzić sprzedaż Oprogramowania Klienckiego Posiadacza Konta wyłącznie przy użyciu ekranu powitalnego Trusteer lub interfejsu API Rapport. Ponadto Klientowi nie wolno wykorzystywać Oprogramowania Klienckiego Posiadacza Konta do wewnętrznej działalności swojego przedsiębiorstwa ani na potrzeby użytkowania przez pracowników Klienta (z wyjątkiem użytku osobistego przez pracowników).

b. Skrypt WWW:

   Skrypt, który umożliwia dostęp do serwisu WWW w celu uzyskania dostępu do ofert IBM SaaS lub korzystania z nich.

c. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane przez Oprogramowanie Klienckie Posiadacza Konta w wyniku elektronicznych interakcji Posiadacza Konta z Aplikacją Biznesową lub Indywidualną, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach ofert IBM SaaS. Otrzymane dane o zdarzeniach będą pochodziły z Oprogramowania Klienckiego Posiadacza Konta działającego na urządzeniach Uprawnionych Uczestników, którzy zaakceptowali warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w Aplikacji Biznesowej lub Indywidualnej Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników.

d. Ekran Powitalny Trusteer:

   Ekran Powitalny Trusteer to platforma marketingowa pozwalająca prezentować i sprzedawać Oprogramowanie Klienckie Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS. Klient może dokonać wyboru spośród dostępnych szablonów Ekranu Powitalnego Trusteer. W ramach odrębnej umowy lub odrębnego zakresu prac można zlecić wykonanie ekranu powitalnego dostosowanego do określonych potrzeb.

Klient może zgodzić się na udostępnienie swoich znaków towarowych, logo lub ikon przeznaczonych do użytku w powiązaniu z Aplikacją TMA. Materiały te będą przeznaczone wyłącznie do używania wraz z Ekranem Powitalnym Trusteer oraz do wyświetlania w Oprogramowaniu Klienckim Posiadacza Konta lub na stronach docelowych udostępnianych przez IBM i w serwisie WWW IBM Security Trusteer. Każde użycie dostarczonych znaków towarowych, logo lub ikon będzie zgodne z uzasadnioną strategią IBM dotyczącą używania materiałów reklamowych i znaków towarowych.

Klient musi dokonać subskrypcji oferty IBM Security Trusteer Rapport Mandatory Service SaaS, jeśli chce zastosować dowolny rodzaj obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

Obowiązek zainstalowania Oprogramowania Klienckiego Posiadacza Konta zachodzi w szczególności w przypadku dowolnego rodzaju obowiązku zainstalowania realizowanego za pomocą jakichkolwiek

mechanizmów lub środków, które bezpośrednio lub pośrednio zmuszają Uprawnionego Uczestnika do pobrania Oprogramowania Klienckiego Posiadacza Konta, lub w przypadku zastosowania metody, narzędzia, procedury, umowy lub mechanizmu, które nie zostały utworzone ani zatwierdzone przez IBM, a powstały w celu obejścia wymagań licencyjnych w stosunku do obowiązkowego instalowania Oprogramowania Klienckiego Posiadacza Konta.

2.2 Dodatkowe opcjonalne oferty IBM SaaS dotyczące usług IBM Security Trusteer Rapport for Business i/lub IBM Security Trusteer Rapport for Retail

W przypadku subskrypcji każdej z poniższych dodatkowych ofert IBM SaaS wymaganiem wstępnym jest subskrypcja ofert IBM Security Trusteer Rapport. Jeśli w nazwie oferty usług IBM SaaS występuje określenie „for Business", to dodatkowa nabywana oferta IBM SaaS również musi być określona w ten sposób. Jeśli w nazwie oferty usług IBM SaaS występuje określenie „for Retail", to dodatkowa nabywana oferta IBM SaaS również musi być określona w ten sposób. Klient będzie otrzymywać dane o zdarzeniach od Uprawnionych Uczestników korzystających z Oprogramowania Klienckiego Posiadacza Konta, którzy zaakceptowali warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w jednej lub wielu Aplikacjach Biznesowych i/lub Indywidualnych Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników.

2.2.1 Oferty IBM Security Trusteer Rapport Fraud Feeds for Business i/lub IBM Security Trusteer Rapport Fraud Feeds for Retail

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach dotyczących zawirusowania szkodliwym oprogramowaniem oraz innych słabych punktów zabezpieczeń w punktach końcowych na komputerze desktop konkretnego Posiadacza Konta.

2.2.2 Oferty IBM Security Trusteer Rapport Phishing Protection for Business i/lub IBM Security Trusteer Rapport Phishing Protection for Retail

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach dotyczących wprowadzania danych uwierzytelniających w serwisach, które mogą być wykorzystywane przez oszustów lub co do których zachodzi podejrzenie, że służą one do wyłudzania informacji. Działające zgodnie z prawem aplikacje online (adresy URL) mogą być pomyłkowo oznaczane jako serwisy służące do wyłudzania informacji. Ponadto usługa IBM SaaS może przesyłać Posiadaczom Konta alerty, w których serwis działający zgodnie z prawem jest określany jako serwis służący do wyłudzania informacji. W takich przypadkach Klient musi powiadamiać IBM o błędach, a IBM zobowiązuje się je naprawiać, przy czym jest to jedyne zadośćuczynienie, jakie przysługuje Klientowi z tytułu zgłoszonego błędu.

2.2.3 Oferty IBM Security Trusteer Rapport Mandatory Service for Business i/lub IBM Security Trusteer Rapport Mandatory Service for Retail

Klient może użyć instancji Ekranu Powitalnego Trusteer stanowiącego platformę marketingową, aby zlecić pobranie Oprogramowania Klienckiego Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS.

W przypadku usługi IBM Security Rapport Mandatory Service for Business wymaganiem wstępnym jest posiadanie usługi IBM Security Trusteer Rapport Premium Support for Business.

W przypadku usługi IBM Security Rapport Mandatory Service for Retail wymaganiem wstępnym jest posiadanie usługi IBM Security Trusteer Rapport Premium Support for Retail.

Klient może zaimplementować dodatkową funkcjonalność usługi IBM Security Trusteer Rapport Mandatory Service tylko pod warunkiem, że została ona zamówiona i skonfigurowana pod kątem używania z Aplikacją Indywidualną lub Biznesową Klienta, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS.

3. Oferty IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint to usługa przetwarzania w chmurze zaprojektowana z myślą o zapewnieniu kolejnej warstwy ochrony. Celem tej usługi jest wykrywanie szkodliwego oprogramowania, przypadków wyłudzania informacji i ataków polegających na przejęciu kontroli nad urządzeniem oraz ograniczanie skutków takich działań. Usługę Trusteer Pinpoint można zintegrować z Biznesowymi i/lub Indywidualnymi Aplikacjami Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony i procesów zapobiegania oszustwom dostępnych w ramach ofert IBM SaaS.

Niniejsza oferta usług IBM SaaS zawiera:

a. Aplikację TMA:

   Aplikacja TMA jest udostępniania w środowisku IBM Security Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków personelu) może: (i) otrzymywać raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać, konfigurować i ustalać strategie bezpieczeństwa oraz strategie związane z raportowaniem danych o zdarzeniach.

b. Skrypt WWW i/lub interfejsy API:

   Narzędzia do zainstalowania w serwisie WWW w celu uzyskania dostępu do oferty IBM SaaS lub korzystania z niej.

3.1 Oferty IBM Security Trusteer Pinpoint Malware Detection oraz IBM Security Trusteer Pinpoint Criminal Detection

W przypadku wykrycia szkodliwego oprogramowania w ramach ofert IBM Security Trusteer Pinpoint Malware Detection lub wykrycia przejęcia konta w ramach ofert IBM Security Trusteer Pinpoint Criminal Detection Klient jest zobowiązany postępować zgodnie z Podręcznikiem sprawdzonych procedur Pinpoint. Z ofert IBM Security Trusteer Pinpoint Malware Detection oraz IBM Security Trusteer Pinpoint Criminal Detection należy korzystać w taki sposób, aby nie wpływać na zachowanie Uprawnionych Uczestników tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta, gdyż mogłoby to umożliwić innym osobom powiązanie czynności wykonanych przez Klienta z użyciem ofert IBM Security Trusteer Pinpoint (np. powiadomienia, komunikaty, blokowanie urządzeń lub blokowanie dostępu do Aplikacji Biznesowej i/lub Indywidualnej tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta).

3.1.1 Oferty IBM Security Trusteer Pinpoint Criminal Detection for Business i/lub IBM Security Trusteer Pinpoint Criminal Detection for Retail

Wykrywanie podejrzanych działań polegających na przejmowaniu konta przez przeglądarki, które łączą się z Aplikacją Biznesową lub Indywidualną. Usługa ta działa bez oprogramowania klienckiego i wykorzystuje mechanizmy pozwalające wykryć identyfikator urządzenia, przypadki wyłudzania informacji oraz kradzież referencji dokonywaną przy użyciu szkodliwego oprogramowania. Usługi IBM Security Trusteer Pinpoint Criminal Detection zapewniają kolejną warstwę ochrony, a ich celem jest wykrywanie prób przejęcia konta. Ponadto dostarczają one bezpośrednio Klientowi (za pośrednictwem przeglądarki rodzimej lub aplikacji Klienta dla urządzeń mobilnych) wyniki oceny ryzyka, jakiemu podlegają przeglądarki i urządzenia mobilne uzyskujące dostęp do Aplikacji Biznesowej lub Indywidualnej.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

3.1.2 Oferty IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile i/lub IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Oferty IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) zapewniają kolejną warstwę ochrony, zabezpieczając przed przejęciem konta i działaniami oszustów przez wykrywanie dostępu do konta w celach przestępczych i generowanie rekomendacji dla Klienta. Usługi IBM SaaS z tej oferty gromadzą informacje pochodzące zarówno z Aplikacji Biznesowej i/lub Indywidualnej Klienta używającej funkcji PPCD Mobile API, jak i z urządzeń mobilnych Uprawnionych Uczestników. Oferty IBM Security Trusteer PPCD przeprowadzają korelację złożonych zestawów informacji dotyczących urządzeń mobilnych Uprawionych Uczestników z danymi z innych źródeł, pochodzącymi między innymi z mechanizmów, które wykrywają w czasie rzeczywistym szkodliwe oprogramowanie oraz incydenty polegające na wyłudzaniu informacji i są zintegrowane za pośrednictwem innych ofert IBM SaaS z grupy IBM Security Trusteer wyszczególnionych w niniejszych Warunkach Używania.

Klient może uzyskiwać dostęp do usług IBM Security Trusteer PPCD Mobile i korzystać z nich w środowisku IBM Security Trusteer udostępnianym w chmurze. Ponadto Klient może otrzymywać dane o ocenie ryzyka wygenerowane w wyniku elektronicznych interakcji urządzeń mobilnych z Aplikacją

Biznesową lub Indywidualną Klienta, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS. Na potrzeby niniejszej oferty pojęcie „urządzenia mobilne" obejmuje wyłącznie obsługiwane telefony komórkowe i tablety, natomiast nie obejmuje komputerów typu PC lub MAC.

3.1.3 Oferty IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Wykrywanie przeglądarek łączących się z Aplikacją Biznesową i/lub Indywidualną, które są zawirusowane szkodliwym oprogramowaniem typu MitB ukierunkowanym na transakcje finansowe (mechanizm ten działa bez oprogramowania klienckiego). Oferty IBM Security Trusteer Pinpoint Malware Detection zapewniają dodatkową warstwę ochrony, a ich celem jest wyposażenie organizacji w narzędzia, które pozwalają koncentrować się na procesach zapobiegania oszustwom opartym na szkodliwym oprogramowaniu. Jest to możliwe dzięki dostarczaniu Klientowi ocen i alertów dotyczących obecności szkodliwego oprogramowania typu MitB ukierunkowanego na transakcje finansowe.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta.

b. Wydanie Advanced Edition:

   Wydania Advanced Edition dla wersji Biznesowej i/lub Indywidualnej oferują dodatkową warstwę ochrony i wykrywania dostosowaną i skorygowaną pod kątem struktury Aplikacji Biznesowych i/lub Indywidualnych Klienta oraz przepływów między nimi. Ponadto wydania te można dostosowywać do konkretnych schematów zagrożeń, jakim podlega Klient, oraz wbudowywać w różne obszary Aplikacji Biznesowych i/lub Indywidualnych Klienta.

   Wydanie Advanced Edition jest oferowane Klientowi przy minimalnej wielkości zamówienia obejmującej 100 tys. Uprawnionych Uczestników wersji Indywidualnej lub 10 tys. Uprawnionych Uczestników wersji Biznesowej, czyli 1000 pakietów po 100 Uprawnionych Uczestników wersji Indywidualnej lub 1000 pakietów po 10 Uprawnionych Uczestników wersji Biznesowej.

c. Wydanie Standard Edition:

   Wydanie Standard Edition dla wersji Biznesowej lub wersji Indywidualnej to przeznaczone do szybkiego wdrożenia rozwiązanie, które zapewnia podstawową funkcjonalność oferty usług IBM SaaS opisanej w niniejszym dokumencie.

3.2 Opcjonalne dodatkowe oferty IBM SaaS dla usług IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition i/lub IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

W przypadku ofert IBM Security Trusteer Rapport Remediation for Retail wymaganiem wstępnym jest subskrypcja oferty IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition lub oferty IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

W przypadku oferty IBM Security Trusteer Pinpoint Carbon Copy for Retail wymaganiem wstępnym jest subskrypcja oferty IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition lub oferty IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. W przypadku ofert IBM Security Trusteer Pinpoint Carbon Copy for Business wymaganiem wstępnym jest subskrypcja oferty IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition lub oferty IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 Oferty IBM Security Trusteer Pinpoint Carbon Copy for Business i/lub IBM Security Trusteer Pinpoint Carbon Copy for Retail

Oferty IBM Security Trusteer Pinpoint Carbon Copy zostały zaprojektowane z myślą o zapewnieniu kolejnej warstwy ochrony oraz usługi monitorowania. Takie rozwiązanie pomaga ustalić, czy bezpieczeństwo referencji Uprawnionego Uczestnika zostało naruszone poprzez ataki mające na celu

wyłudzanie informacji w Aplikacjach Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach ofert IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

Celem usługi IBM Security Trusteer Rapport Remediation for Retail jest zbadanie, zneutralizowanie, zablokowanie i usunięcie szkodliwego oprogramowania typu MitB z zawirusowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy doraźnie uzyskują dostęp do Aplikacji Indywidualnej Klienta. Wykryte przypadki zawirusowania szkodliwym oprogramowaniem są uwzględniane w danych o zdarzeniach dostarczanych przez usługę IBM Security Trusteer Pinpoint Malware Detection. Klient musi posiadać bieżącą subskrypcję usługi IBM Security Trusteer Pinpoint Malware Detection działającej w danym momencie wraz z Aplikacją Indywidualną Klienta. Klient może korzystać z niniejszej oferty IBM SaaS wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Indywidualnej Klienta. Ponadto niniejsza oferta IBM SaaS może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Security Trusteer Rapport Remediation for Retail musi działać na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub wielu Aplikacjach Indywidualnych Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza oferta IBM SaaS nie obejmuje prawa do używania Ekranu Powitalnego Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta.

4. Oferty IBM Security Trusteer Mobile

4.1 Oferty IBM Security Trusteer Mobile Browser for Business i/lub IBM Security Trusteer Mobile Browser for Retail

Oferta IBM Security Trusteer Mobile Browser została zaprojektowana z myślą o wprowadzeniu kolejnej warstwy ochrony, a jej celem jest zapewnienie bezpieczeństwa podczas dostępu uzyskiwanego za pośrednictwem mobilnych urządzeń Uprawnionych Uczestników do Aplikacji Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji oferty usług IBM SaaS w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android. Niniejsza oferta IBM SaaS dla urządzeń mobilnych obejmuje telefony komórkowe i tablety, lecz nie obejmuje laptopów typu PC i Mac.

Dzięki Aplikacji TMA Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może otrzymywać dane o zdarzeniach, analizy i informacje statystyczne dotyczące Urządzeń będących w posiadaniu Uprawnionych Uczestników, którzy: (i) pobrali Oprogramowanie Klienckie Posiadacza Konta, czyli aplikację podlegającą bezpłatnej publicznej licencji na warunkach Umowy Licencyjnej z Użytkownikiem Końcowym, udostępnianą do pobrania na urządzenia mobilne Uprawnionych Uczestników, oraz (ii) zaakceptowali Umowę Licencyjną z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnili się w Aplikacjach Indywidualnych lub Biznesowych Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach ofert IBM SaaS. Klient może prowadzić sprzedaż Oprogramowania Klienckiego Posiadacza Konta wyłącznie przy użyciu Ekranu Powitalnego Trusteer. Ponadto Klientowi nie wolno wykorzystywać Oprogramowania Klienckiego Posiadacza Konta do wewnętrznej działalności swojego przedsiębiorstwa.

a. Dane o zdarzeniach:

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji urządzeń mobilnych z Aplikacjami Indywidualnymi lub Biznesowymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS.

b. Ekran Powitalny Trusteer:

   Ekran Powitalny Trusteer to platforma marketingowa pozwalająca prezentować i sprzedawać Oprogramowanie Klienckie Posiadacza Konta Uprawnionym Uczestnikom uzyskującym dostęp do Aplikacji Biznesowych i/lub Indywidualnych, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS. Klient może dokonać wyboru spośród dostępnych szablonów Ekranu Powitalnego Trusteer („Szablon Ekranu Powitalnego”). W ramach odrębnej

umowy lub odrębnego zakresu prac można zlecić wykonanie ekranu powitalnego dostosowanego do określonych potrzeb.

Klient może zgodzić się na udostępnienie swoich znaków towarowych, logo lub ikon przeznaczonych do użytku w powiązaniu z Aplikacją TMA. Materiały te będą przeznaczone wyłącznie do używania wraz z Ekranem Powitalnym Trusteer oraz do wyświetlania w Oprogramowaniu Klienckim Posiadacza Konta, na stronach docelowych udostępnianych przez IBM, albo w serwisie WWW IBM Security Trusteer. Każde użycie dostarczonych znaków towarowych, logo lub ikon będzie zgodne z uzasadnioną strategią IBM dotyczącą używania materiałów reklamowych i znaków towarowych.

4.2 Oferty IBM Security Trusteer Mobile SDK for Business i/lub IBM Security Trusteer Mobile SDK for Retail

Oferty IBM Security Trusteer Mobile SDK zostały zaprojektowane z myślą o wprowadzeniu kolejnej warstwy ochrony, tak aby zapewnić bezpieczny dostęp w sieci WWW do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji ofert IBM SaaS w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji metodą pharming. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android.

Usługi IBM Security Trusteer Mobile SDK zawierają prawnie zastrzeżony pakiet narzędzi do tworzenia oprogramowania dla urządzeń mobilnych („SDK"). Jest to pakiet oprogramowania zawierający dokumentację, prawnie zastrzeżone biblioteki programistyczne oraz inne powiązane pliki i elementy określane nazwą „biblioteka IBM Security Trusteer dla urządzeń mobilnych", a także „komponent środowiska wykonawczego" lub „Element Podlegający Redystrybucji", czyli prawnie zastrzeżony kod wygenerowany przez pakiet IBM Security Trusteer Mobile SDK, który można osadzać w autonomicznych, chronionych aplikacjach Klienta dla urządzeń mobilnych z systemem operacyjnym iOS lub Android (oraz integrować z takimi aplikacjami), w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach usługi IBM SaaS („Zintegrowana przez Klienta Aplikacja dla Urządzeń Mobilnych").

Oferta IBM Security Trusteer Mobile SDK for Retail jest dostępna w pakietach po 100 Uprawnionych Uczestników lub w pakietach po 100 Urządzeń Klienckich, natomiast oferta IBM Security Trusteer Mobile SDK for Business jest dostępna w pakietach po 10 Uprawnionych Uczestników lub w pakietach po 10 Urządzeń Klienckich.

Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może uzyskiwać za pośrednictwem aplikacji TMA dane o zdarzeniach i oceny trendów ryzyka. Klient może odbierać za pośrednictwem Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych informacje dotyczące analizy ryzyka i urządzeń mobilnych w odniesieniu do urządzeń Uprawnionych Uczestników, którzy pobrali Zintegrowaną przez Klienta Aplikację dla Urządzeń Mobilnych. Pozwala to Klientowi opracować strategię zapobiegania oszustwom w celu egzekwowania działań zmierzających do ograniczenia skutków takiego ryzyka. Na potrzeby niniejszej oferty pojęcie „urządzenia mobilne" obejmuje wyłącznie obsługiwane telefony komórkowe i tablety, natomiast nie obejmuje komputerów typu PC lub MAC.

Klient może:

a. wykorzystywać pakiet IBM Security Trusteer Mobile SDK do użytku wewnętrznego, wyłącznie na potrzeby opracowywania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych;

b. osadzić Element Podlegający Redystrybucji (wyłącznie w postaci kodu wynikowego) w Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, tak aby stanowił on integralną, nieodłączną część tej aplikacji. Każdy fragment Elementu Podlegającego Redystrybucji zmodyfikowany lub wbudowany zgodnie z niniejszą licencją będzie podlegał niniejszym Warunkom Używania;

c. prowadzić sprzedaż i dystrybucję Elementu Podlegającego Redystrybucji przeznaczonego do pobrania na urządzenia mobilne Uprawnionych Uczestników lub do pobrania przez posiadacza Urządzenia Klienckiego, pod warunkiem że:

   - Z wyjątkiem przypadków wyraźnie dozwolonych w niniejszej Umowie, Klient nie ma prawa (1) używać, kopiować, modyfikować ani dystrybuować pakietu SDK; (2) deasemblować, dekompilować ani przeprowadzać translacji pakietu SDK innymi metodami (z wyjątkiem przypadków wyraźnie dozwolonych przez przepisy prawa bez możliwości ich wyłączenia w ramach umowy); (3) udzielać dalszych licencji, wypożyczać lub wydzierżawiać pakietu SDK; (4) usuwać żadnych plików z informacjami o prawach autorskich ani plików informacyjnych zawartych w Elemencie Podlegającym Redystrybucji; (5) używać tej samej nazwy ścieżki,

która została użyta w oryginalnych plikach/modułach Elementu Podlegającego Redystrybucji; (6) używać nazw ani znaków towarowych IBM oraz jego licencjodawców i dystrybutorów w powiązaniu ze sprzedażą Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych bez uprzedniej pisemnej zgody IBM lub odpowiedniego licencjodawcy bądź dystrybutora.

- Element Podlegający Redystrybucji musi pozostać nierozłącznie zintegrowany ze Zintegrowaną przez Klienta Aplikacją dla Urządzeń Mobilnych; ponadto musi mieć wyłącznie postać kodu wynikowego i spełniać wszystkie wytyczne, instrukcje i specyfikacje zawarte w pakiecie SDK i jego dokumentacji. Umowa licencyjna z użytkownikiem końcowym Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych musi zawierać zapis informujący użytkownika końcowego, że Elementu Podlegającego Redystrybucji nie wolno i) używać do jakichkolwiek innych celów niż umożliwienie działania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, ii) kopiować (z wyjątkiem tworzenia kopii zapasowej), iii) przeznaczać do dalszej dystrybucji lub przekazywać, iv) deasemblować, dekompilować ani w inny sposób poddawać translacji, o ile nie zezwalają na to przepisy prawa bez możliwości ich wyłączenia w ramach umowy. Umowa licencyjna zawarta przez Klienta musi chronić prawa IBM w stopniu co najmniej równoważnym warunkom niniejszej Umowy.
- Pakiet SDK może być wdrażany tylko w ramach wewnętrznych testów programistycznych i jednostkowych prowadzonych przez Klienta na urządzeniach mobilnych określonych przez Klienta jako testowe. Klient nie jest upoważniony do używania pakietu SDK w celu przetwarzania lub symulowania obciążeń produkcyjnych ani testowania skalowalności jakiegokolwiek kodu, programu lub systemu. Klient nie jest uprawniony do używania jakiejkolwiek części pakietu SDK do innych celów.

Klient odpowiada za świadczenie pełnego zakresu usług pomocy technicznej w odniesieniu do Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz wszelkich modyfikacji w Elemencie Podlegającym Redystrybucji, wprowadzonych przez Klienta w sposób dozwolony w niniejszym dokumencie.

Klient może zainstalować Elementy Podlegające Redystrybucji oraz pakiet IBM Security Mobile SDK i używać ich wyłącznie w celu ułatwienia sobie korzystania z oferty usług IBM SaaS.

IBM przetestował przykładowe aplikacje utworzone za pomocą narzędzi mobilnych udostępnionych w pakiecie IBM Security Trusteer Mobile SDK („Narzędzia Mobilne”), aby ustalić, czy aplikacje te będą się poprawnie uruchamiały na niektórych wersjach mobilnych platform systemów operacyjnych firm Apple (iOS), Google (Android) oraz innych dostawców (zwanych łącznie „Mobilnymi Platformami Systemów Operacyjnych”). Mobilne Platformy Systemów Operacyjnych są jednak udostępniane przez osoby trzecie, nie podlegają kontroli IBM i mogą ulec zmianie bez powiadamiania IBM. Dlatego bez względu na stanowiące inaczej warunki IBM nie gwarantuje, że jakiekolwiek aplikacje lub inne produkty utworzone za pomocą Narzędzi Mobilnych będą poprawnie uruchamiać się na jakichkolwiek Mobilnych Platformach Systemów Operacyjnych lub urządzeniach mobilnych, ani też że będą z nimi współdziałać lub że będą z nimi zgodne.

Klient zobowiązuje się utworzyć, przechowywać i udostępnić IBM oraz jego rewidentom dokładne rejestry pisemne, dane wyjściowe narzędzi systemowych oraz inne informacje systemowe, wystarczające do stwierdzenia, że korzystanie przez Klienta z pakietu IBM Security Trusteer Mobile SDK odbywa się zgodnie z niniejszymi Warunkami Używania.

5. Wdrażanie ofert IBM SaaS do ochrony przed oszustwami

Podstawowa subskrypcja Klienta obejmuje wymagane czynności z zakresu konfigurowania i początkowego instalowania, w tym jednorazowe początkowe uruchamianie, konfigurowanie, dostarczanie Szablonu Ekranu Powitalnego, testowanie i szkolenie.

Dodatkowe usługi mogą zostać zlecone za dopłatą w ramach odrębnej umowy.

Dodatek B

Niniejsza Umowa dotycząca Poziomu Usług w zakresie dostępności odnosi się do usługi IBM SaaS i ma zastosowanie pod warunkiem wyszczególnienia jej w Dokumencie Transakcyjnym Klienta;

przy czym wersją obowiązującą jest wersja aktualna w momencie rozpoczęcia lub odnowienia okresu subskrypcji Klienta. Jednocześnie Klient uznaje, że Umowa dotycząca Poziomu Usług nie stanowi gwarancji udzielonej Klientowi (rękojmia jest niniejszym również wyłączona).

1. Definicje

a. **Upoważniona Osoba Kontaktowa** — osoba wskazana IBM przez Klienta, która jest upoważniona do składania Reklamacji na mocy niniejszej Umowy dotyczącej Poziomu Usług.

b. **Uznanie z tytułu Dostępności** — zadośćuczynienie dokonywane przez IBM w związku z potwierdzoną Reklamacją. Uznanie z tytułu Dostępności może mieć postać uznania lub upustu na poczet przyszłej faktury z tytułu opłat za subskrypcję usługi IBM SaaS.

c. **Reklamacja** — roszczenie składane przez Upoważnioną Osobę Kontaktową ze strony Klienta na ręce IBM zgodnie z niniejszą Umową dotyczącą Poziomu Usług, które dotyczy niedotrzymania Poziomu Usług w określonym Miesiącu Obowiązywania Umowy.

d. **Miesiąc Obowiązywania Umowy** — pełny miesiąc w okresie świadczenia Usługi IBM SaaS, liczony od godziny 0:00 czasu GMT w pierwszym dniu miesiąca do godziny 23:59 czasu GMT w ostatnim dniu miesiąca.

e. **Klient** — podmiot subskrybujący usługę IBM SaaS bezpośrednio od IBM, który nie narusza żadnych istotnych zobowiązań wynikających z umowy z IBM dotyczącej usługi IBM SaaS, w tym zobowiązań w zakresie płatności.

f. **Przestój** — okres, w którym przetwarzanie związane z Usługą w systemie produkcyjnym zostaje wstrzymane, a żaden z użytkowników Klienta nie może korzystać ze wszystkich elementów Usługi, w odniesieniu do których ma odpowiednie uprawnienia. Za Przestój nie uznaje się okresu, w którym Usługa jest niedostępna z powodu:

- Planowego Przestoju Systemu;
- działania Siły Wyższej;
- problemów związanych z aplikacjami, urządzeniami lub danymi Klienta bądź osób trzecich;
- działań lub zaniechań ze strony Klienta lub osób trzecich (w tym uzyskania przez jakąkolwiek osobę dostępu do usługi IBM SaaS przy użyciu haseł lub urządzeń Klienta);
- nieprzestrzegania wymagań dotyczących konfiguracji systemu i obsługiwanych platform służących do korzystania z usługi IBM SaaS;
- zastosowania się IBM do projektów, specyfikacji lub instrukcji dostarczonych przez Klienta lub osobę trzecią w imieniu Klienta.

g. **Zdarzenie** — okoliczność lub splot okoliczności, które powodują niedotrzymanie Poziomu Usług.

h. **Siła Wyższa** — zdarzenia losowe, akty terroru, strajki, pożary, powodzie, trzęsienia ziemi, zamieszki, wojny, ustawy, nakazy lub ograniczenia ustanawiane przez organy administracji publicznej, wirusy, ataki polegające na spowodowaniu odmowy usługi i inne szkodliwe działania, awarie infrastruktury komunalnej i połączeń sieciowych bądź inne okoliczności powodujące niedostępność usługi IBM SaaS, na które IBM nie ma wpływu.

i. **Planowany Przestój Systemu** — planowane wyłączenie Usługi IBM SaaS związane z jej konserwacją.

j. **Poziom Usług** — określony poniżej standard, zgodnie z którym IBM mierzy poziom usług świadczonych w ramach niniejszej Umowy dotyczącej Poziomu Usług.

2. Uznania z tytułu Dostępności

a. Aby nabyć prawo do złożenia Reklamacji, Klient musi wcześniej zarejestrować w dziale obsługi klienta IBM zgłoszenie problemu dotyczące każdego Zdarzenia związanego z daną usługą IBM SaaS (zgodnie z określoną przez IBM procedurą zgłaszania problemów o poziomie istotności 1). Klient ma przy tym obowiązek podać wszelkie niezbędne, szczegółowe informacje na temat Zdarzenia oraz udzielić IBM należytej pomocy przy diagnozowaniu i rozwiązywaniu problemu będącego przyczyną takiego Zdarzenia w zakresie wymaganym w przypadku zgłoszeń o poziomie istotności 1. Ponadto zgłoszenie musi zostać zarejestrowane w ciągu 24 (dwudziestu czterech) godzin od momentu uzyskania przez Klienta informacji o tym, że dane Zdarzenie wpłynęło na korzystanie przez Klienta z usługi IBM SaaS.

b. Upoważniona Osoba Kontaktowa ze strony Klienta musi złożyć Reklamację z wnioskiem o dokonanie Uznania z tytułu Dostępności nie później niż w ciągu 3 (trzech) dni roboczych od końca Miesiąca Obowiązywania Umowy, którego dotyczy taka Reklamacja.

c. Upoważniona Osoba Kontaktowa ze strony Klienta musi podać IBM wszelkie wymagane w uzasadnionym zakresie informacje związane z Reklamacją, a w szczególności dokładny opis wszelkich Zdarzeń oraz określenie Poziomu Usług, który zdaniem Klienta nie został dotrzymany.

d. IBM będzie prowadzić wewnętrzne pomiary łącznego czasu trwania Przestojów w każdym Miesiącu Obowiązywania Umowy w odniesieniu do stosownego Poziomu Usług wskazanego w poniższej tabeli. Uznania z tytułu Dostępności będą zależeć od czasu trwania Przestojów mierzonego od daty i godziny zgłoszenia pierwszego wystąpienia Przestoju. Jeśli Klient zgłosi jednocześnie Zdarzenie Przestoju Aplikacji oraz Zdarzenie Przestoju Przetwarzania Danych Przychodzących, IBM potraktuje nakładające się okresy Przestoju jako jeden i ten sam okres Przestoju, a nie jako dwa oddzielne okresy Przestoju. W przypadku każdej uzasadnionej Reklamacji IBM naliczy najwyższe obowiązujące Uznanie z tytułu Dostępności na podstawie osiągniętego Poziomu Usług w danym Miesiącu Obowiązywania Umowy, zgodnie z poniższymi tabelami. Jednocześnie zastrzega się, że IBM nie ma obowiązku dokonywania kilku Uznań z tytułu Dostępności w związku z tym samym Zdarzeniem w tym samym Miesiącu Obowiązywania Umowy.

e. W przypadku Usługi Pakietowej (czyli usług IBM SaaS połączonych w pakiet i sprzedawanych razem za jedną cenę) Uznanie z tytułu Dostępności będzie obliczane na podstawie łącznej ceny takiej Usługi Pakietowej, nie zaś na podstawie miesięcznych opłat za subskrypcję poszczególnych usług IBM SaaS. Klient może składać w każdym Miesiącu Obowiązywania Umowy Reklamacje dotyczące tylko jednej usługi IBM SaaS wchodzącej w skład pakietu, a IBM nie ma obowiązku dokonywania Uznań z tytułu Dostępności dotyczących więcej niż jednej usługi IBM SaaS wchodzącej w skład pakietu w każdym Miesiącu Obowiązywania Umowy.

f. Jeśli Klient nabył usługę IBM SaaS u autoryzowanego resellera IBM w ramach transakcji odsprzedaży, w przypadku której IBM ponosi podstawową odpowiedzialność za wypełnianie zobowiązań związanych z usługą IBM SaaS i Umową dotyczącą Poziomu Usług, Uznanie z tytułu Dostępności zostanie obliczone na podstawie obowiązującej w danym momencie ceny RSVP (Relationship Suggested Value Price) usługi IBM SaaS za Miesiąc Obowiązywania Umowy, którego dotyczy Reklamacja, objętej upustem w wysokości 50%.

g. Łączna wysokość Uznań z tytułu Dostępności przyznawanych za każdy Miesiąc Obowiązywania Umowy nie może w żadnym razie przekroczyć dziesięciu procent (10%) sumy równej jednej dwunastej (1/12) rocznej opłaty za usługę IBM SaaS uiszczanej przez Klienta na rzecz IBM.

h. IBM będzie sprawdzać zasadność Reklamacji z dołożeniem należytej staranności na podstawie informacji dostępnych w dokumentacji IBM, przy czym informacje takie będą miały znaczenie rozstrzygające w przypadku sprzeczności z informacjami zawartymi w dokumentacji Klienta.

i. UZNANIA Z TYTUŁU DOSTĘPNOŚCI PRZYZNAWANE KLIENTOWI ZGODNIE Z NINIEJSZĄ UMOWĄ DOTYCZĄCĄ POZIOMU USŁUG STANOWIĄ WYŁĄCZNE ZADOŚĆUCZYNIENIE PRZYSŁUGUJĄCE KLIENTOWI W ZWIĄZKU ZE WSZELKIMI REKLAMACJAMI.

3. Poziomy Usług

Dostępność usługi IBM SaaS w Miesiącu Obowiązywania Umowy

Osiągnięty Poziom Usług (w Miesiącu Obowiązywania Umowy)	**Uznanie z tytułu Dostępności (procent miesięcznej opłaty za subskrypcję za Miesiąc Obowiązywania Umowy, którego dotyczy Reklamacja)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

„Osiągnięty Poziom Usług" wyrażony procentowo jest równy ilorazowi (a) łącznej liczby minut w danym Miesiącu Obowiązywania Umowy pomniejszonej o (b) łączny czas trwania Przestojów w minutach w danym Miesiącu Obowiązywania Umowy oraz (c) łącznej liczby minut w danym Miesiącu Obowiązywania Umowy.

Przykład: łączny czas trwania Przestojów w Miesiącu Obowiązywania Umowy = 250 minut

43 200 minut w 30-dniowym Miesiącu Obowiązywania Umowy - 250 minut Przestojów = 42 950 minut _____ łącznie 43 200 minut	= 2% Uznanie z tytułu Osiągniętego Poziomu Usług na poziomie 99,4% w Miesiącu Obowiązywania Umowy

3.1 Zastrzeżenia

Niniejsza Umowa dotycząca Poziomu Usług jest dostępna wyłącznie dla Klientów IBM. Ponadto nie ma ona zastosowania w przypadku:

- Usług w wersji beta i Usług świadczonych w okresie próbnym;
- środowisk nieprodukcyjnych, a w szczególności takich zastosowań jak testowanie, usuwanie skutków awarii, zapewnianie jakości i programowanie;
- reklamacji składanych przez użytkowników, odwiedzających, uczestników czy zatwierdzonych gości Klienta IBM korzystających z usługi IBM SaaS;
- naruszenia przez Klienta istotnych zobowiązań wynikających z Warunków Używania, a w szczególności wszelkich zobowiązań dotyczących płatności.