

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

IBM MobileFirst Protect (SaaS)

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 (zwaną 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:

- IBM MobileFirst Protect – Devices (SaaS)
- IBM MobileFirst Protect – Devices (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Applications (SaaS)
- IBM MobileFirst Protect – Applications (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Application Security (SaaS)
- IBM MobileFirst Protect – Application Security (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Gateway for Apps (SaaS)
- IBM MobileFirst Protect – Gateway for Apps (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Content (SaaS)
- IBM MobileFirst Protect – Content (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Document Sync (SaaS)
- IBM MobileFirst Protect – Document Sync (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Document Editor (SaaS)
- IBM MobileFirst Protect – Document Editor (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Gateway for Documents (SaaS)
- IBM MobileFirst Protect – Gateway for Documents (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Email Management (SaaS)
- IBM MobileFirst Protect – Email Management (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Browser (SaaS)
- IBM MobileFirst Protect – Browser (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Gateway for Browser (SaaS)
- IBM MobileFirst Protect – Gateway for Browser w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect for Blackberry (SaaS)
- IBM MobileFirst Protect for Blackberry (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Expenses (SaaS)
- IBM MobileFirst Protect – Expenses (SaaS) w wersji Step Up dla dotychczasowych klientów

- IBM MobileFirst Protect – Management Suite (SaaS)
- IBM MobileFirst Protect – Management Suite (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Productivity Suite (SaaS)
- IBM MobileFirst Protect – Productivity Suite (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Secure Mail (SaaS)
- IBM MobileFirst Protect – Secure Mail (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Gateway Suite (SaaS)
- IBM MobileFirst Protect – Gateway Suite (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Content Suite (SaaS)
- IBM MobileFirst Protect – Content Suite (SaaS) w wersji Step Up dla dotychczasowych klientów
- IBM MobileFirst Protect – Threat Management (SaaS)
- IBM MobileFirst Protect – Content Service (SaaS)
- IBM MobileFirst Protect – Content Service Storage (SaaS)
- IBM MobileFirst Protect – Content Service Bandwidth (SaaS)
- IBM MobileFirst Protect – Professional (SaaS)
- IBM MobileFirst Protect – Laptop (SaaS)
- IBM MobileFirst Protect – Laptop Location (SaaS)
- IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)
- IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)
- IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)
- IBM MaaS360 Secure Productivity Suite Prime (SaaS)
- IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)
- IBM MaaS360 Professional Bundle Prime (SaaS)
- IBM MaaS360 Educational Bundle Prime (SaaS)
- IBM MaaS360 Advanced Laptop Management Prime (SaaS)

2. Opłaty rozliczeniowe

Przy sprzedaży usługi IBM SaaS wysokość opłat rozliczeniowych jest ustalana na podstawie następujących miar określonych w Dokumencie Transakcyjnym:

- a. Jednostką miary, według której można korzystać z usługi IBM SaaS, jest **Autoryzowany Użytkownik**. Klient musi uzyskać oddzielne, dedykowane uprawnienia dla każdego unikalnego Autoryzowanego Użytkownika, który otrzymuje dostęp do usługi IBM SaaS w jakolwiek sposób, bezpośrednio lub pośrednio (na przykład przez program multipleksujący, urządzenie lub serwer aplikacji), przy użyciu dowolnych środków. Ponadto Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę stosownej liczby Autoryzowanych Użytkowników otrzymujących dostęp do usługi IBM SaaS w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym Klienta.
- b. Jednostką miary, według której można korzystać z usługi IBM SaaS, jest **Gigabajt**. Gigabajt definiuje się jako 2 do 30 potęgi bajtów danych (1 073 741 824 bajtów). Klient musi uzyskać odpowiednie uprawnienia umożliwiające obsługę łącznej liczby Gigabajtów przetwarzanych w ramach usługi IBM SaaS w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym Klienta.
- c. Jednostką miary, według której można korzystać z usług IBM SaaS, jest **Zarządzane Urządzenie Klientkie**. Urządzenie Klientkie 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 Klientkich może współużytkować dostęp do jednego serwera. Aby umożliwić użytkownikowi wykonywanie pracy, Urządzenie Klientkie może być

programowalne lub wyposażone w funkcje przetwarzania. Klient musi uzyskać uprawnienia dla Zarządzanego Urządzenia Klientckiego w odniesieniu do wszystkich Urządzeń Klientckich zarządzanych za pomocą usługi IBM SaaS w okresie pomiarowym określonym w dokumencie Proof of Entitlement (PoE) lub Dokumencie Transakcyjnym Klienta.

- d. Jednostką miary, według której można korzystać z usług IBM SaaS, jest **Urządzenie Klientckie**. Urządzenie Klientckie 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 Klientckich może współużytkować dostęp do jednego serwera. Aby umożliwić użytkownikowi wykonywanie pracy, Urządzenie Klientckie może być programowalne lub wyposażone w funkcje przetwarzania. Klient musi uzyskać uprawnienia dla każdego Urządzenia Klientckiego, które uruchamia rozwiązanie IBM SaaS, dostarcza do niego dane, korzysta z udostępnianych przez nie usług lub w inny sposób uzyskuje do niego dostęp w okresie pomiarowym wyszczególnionym w dokumencie Proof of Entitlement (PoE) lub 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.

3.2 Opłaty za przekroczenie limitu

Jeśli rzeczywiste wykorzystanie usługi IBM SaaS przez Klienta w okresie pomiarowym przekroczy uprawnienia określone w dokumencie PoE, Klientowi zostanie wystawiona zgodnie z postanowieniami Dokumentu Transakcyjnego faktura za przekroczenie limitu.

4. Możliwości odnowienia Okresu Subskrypcji usługi IBM SaaS

W dokumencie PoE Klienta zostanie wskazane, czy usługa IBM SaaS będzie odnawiana z końcem okresu subskrypcji. Poniżej opisano dostępne opcje.

4.1 Automatyczne odnowienie

Jeśli w dokumencie PoE Klienta wskazano, że odnowienie następuje automatycznie, Klient może zrezygnować z usługi IBM SaaS przed końcem dotychczasowego okresu subskrypcji poprzez 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 PoE. 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 określone w dokumencie PoE.

ODNOWIENIE BĘDZIE OBEJMOWAĆ TAKĄ SAMĄ LUB WIĘKSZĄ LICZBĘ UPRAWNIENI, CO PIERWOTNE ZAMÓWIENIE, ALBO LICZBĘ UPRAWNIENI WYNIKAJĄCĄ ZE ZGŁASZANEGO MIESIĘCZNEGO WYKORZYSTANIA W MIESIĄCU POPRZEDZAJĄCYM WYSTAWIENIE FAKTURY ZA ODNOWIENIE, CHYBA ŻE IBM OTRZYMA POWIADOMIENIE OKREŚLAJĄCE INNĄ LICZBĘ UPRAWNIENI DO ODNOWIENIA.

ODNOWIENIE OFERTY TYPU STEP-UP BĘDZIE OBEJMOWAĆ TAKĄ SAMĄ LICZBĘ UPRAWNIENI CO PIERWOTNE ZAMÓWIENIE.

4.2 Rozliczanie ciągle

Jeśli w Dokumencie PoE 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.

4.3 Wymagane odnowienie

Jeśli w dokumencie PoE 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.

5. Wsparcie Techniczne

Wsparcie techniczne udostępniane do usługi IBM SaaS w okresie subskrypcji ma charakter drugiego poziomu wsparcia, co oznacza, że jest dostępne dla zespołu operacyjnego Klienta, ale nie dla jego Użytkowników Końcowych.

Wsparcie jest świadczone różnymi kanałami, przez całą dobę i we wszystkie dni tygodnia (24x7). Informacje dotyczące wsparcia do rozwiązywania IBM SaaS można znaleźć w portalu produktu.

Docelowe założenia dotyczące oczekiwanej szybkości reakcji:

Poziom istotności	Definicja poziomu istotności	Początkowe Docelowe czasy reakcji	Zakres czasu reakcji
1	Krytyczne zakłócenie działalności / uniemożliwienie świadczenia usług: Newralgiczne funkcje biznesowe nie działają lub nastąpiła awaria newralgicznego interfejsu. Zwykle dotyczy to środowiska produkcyjnego i uniemożliwia dostęp do usług, co powoduje krytyczne zakłócenia w działalności gospodarczej. Sytuacja taka wymaga natychmiastowego rozwiązania.	30 minut	24x7
2	Duże zakłócenie działalności: Korzystanie z funkcji usługowych lub działanie usług zostało poważnie ograniczone lub istnieje ryzyko niedotrzymania ważnych terminów.	1 godzina robocza	24x7
3	Średnie zakłócenie działalności: Usługi lub funkcje mogą być używane, a problem nie powoduje krytycznego zakłócenia działalności.	2 godziny robocze	24x7
4	Niewielkie zakłócenie działalności: Zapytanie lub prośba nietechniczna.	3 godziny robocze	24x7

6. Warunki dodatkowe dla oferty usług IBM SaaS

6.1 Ograniczenia dotyczące wersji Step Up

Oferty IBM SaaS określone jako „wersja Step Up dla obecnych Klientów” („usługa SaaS w wersji Step Up”) są przeznaczone wyłącznie dla Klientów, który uprzednio lub równocześnie nabyli odpowiednie uprawnienia licencyjne do powiązanego programu IBM wskazanego w nazwie oferty usług SaaS w wersji Step Up. Na przykład Klient, który nabywa usługę „IBM MobileFirst Protect – Devices (SaaS) – wersja Step Up dla obecnych Klientów”, musi dysponować uprawnieniami licencyjnymi do powiązanego programu, którym jest IBM MobileFirst Protect. Uprawnienia Klienta do usługi SaaS w wersji Step Up nie mogą wykraczać swoim zakresem poza uprawnienia Klienta do powiązanego programu IBM.

W przypadku nabycia usługi SaaS w wersji Step Up Klient nie może używać tych samych uprawnień licencyjnych w odniesieniu do powiązanego programu IBM w środowisku lokalnym oraz w odniesieniu do usługi SaaS w wersji Step Up. Na przykład jeśli Klient posiada 250 uprawnień do Zarządzanych Urządzeń Klientkich na powiązany program IBM i nabydzie 100 uprawnień do Zarządzanych Urządzeń Klientkich w wersji Step Up, to może zarządzać 100 takimi urządzeniami w środowisku Usługi IBM SaaS w ramach oferty Step Up oraz 150 urządzeniami w ramach uprawnień do oprogramowania zainstalowanego lokalnie.

Klient oświadcza, że nabył odpowiednie (1) uprawnienia licencyjne oraz (2) Subskrypcję i Wsparcie dla powiązanych programów IBM. W Okresie Subskrypcji usługi SaaS w wersji Step Up Klient musi zapewnić aktualność Subskrypcji i Wsparcia dla uprawnień do programów IBM używanych w połączeniu z uprawnieniami do usługi SaaS w wersji Step Up. Klient traci prawo do używania usługi SaaS w wersji Step Up w momencie wygaśnięcia licencji Klienta na używanie powiązanych programów IBM lub rozwiązania Subskrypcji i Wsparcia dla powiązanych programów IBM.

6.2 Informacje cookie

Klient zgadza się, że IBM może używać informacji cookie i technik śledzenia w celu zbierania danych osobowych podczas gromadzenia statystyk używania i informacji służących do doskonalenia warunków pracy użytkownika i/lub dostosowania interakcji z użytkownikami zgodnie z zasadami określonymi na stronie <http://www-01.ibm.com/software/info/product-privacy/index.html>.

6.3 Przekazywanie danych za granicę

W przypadku udostępniania Danych Osobowych przez Klienta w ramach ofert IBM SaaS w krajach członkowskich Unii Europejskiej, a także w Islandii, Liechtensteinie, Norwegii, Szwajcarii i Turcji oraz pozostałych państwach europejskich, w których zostały uchwalone miejscowe przepisy dotyczące ochrony danych, Klient wyraża zgodę na przetwarzanie przez IBM Treści (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:

Nazwa podmiotu przetwarzającego / podwykonawcy przetwarzania	Rola (przetwarzający lub podwykonawca przetwarzania)	Lokalizacja
IBM Corporation	Podwykonawca przetwarzania	1 New Orchard Rd. Armonk, NY 10504, Stany Zjednoczone I
IBM India Private Limited	Podwykonawca przetwarzania	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029, Indie

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.

6.4 Ochrona danych w Unii Europejskiej

Jeśli Klient udostępni dane osobowe w ramach ofert IBM SaaS w krajach członkowskich Unii Europejskiej, w Islandii, Liechtensteinie, Norwegii, Szwajcarii, Turcji lub innym kraju europejskim, w którym zostały uchwalone miejscowe przepisy dotyczące ochrony danych, lub jeśli w krajach tych znajdują się autoryzowani użytkownicy bądź urządzenia 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 oferty IBM SaaS zgodnie z opublikowanymi przez IBM opisami usługi IBM SaaS, a Klient potwierdza, że przetwarzanie to jest zawsze zgodne z jego instrukcjami.

6.5 Zgodność z programem Safe Harbor

Oferty usług IBM SaaS są objęte certyfikatem Safe Harbor Stany Zjednoczone–Unia Europejska, uzyskanym przez firmę Fiberlink Communications Corporation (przedsiębiorstwo podporządkowane IBM). IBM oraz Fiberlink przestrzegają w tym zakresie zasad określonych przez Departament Handlu Stanów Zjednoczonych w ramach programu US–EU Safe Harbor Framework, które regulują sposób gromadzenia, wykorzystywania i przechowywania informacji pochodzących z Unii Europejskiej. Więcej informacji na temat programu Safe Harbor, w tym oświadczenie Fiberlink dotyczące certyfikacji, można znaleźć pod adresem <http://www.export.gov/safeharbor/>.

Jeśli przekazanie Danych Osobowych z terytorium Europejskiej Strefy Ekonomicznej nie jest objęte programem Safe Harbor Stany Zjednoczone–Unia Europejska, 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.

6.6 Miejsce osiągnięcia korzyści pochodnych

Podatki, o ile mają zastosowanie, są oparte na miejscu lub miejscach, które Klient określi jako miejsca osiągnięcia korzyści z usługi IBM SaaS. IBM będzie stosować podatki na podstawie adresu działalności, który Klient poda podczas zamawiania usługi IBM SaaS jako główne miejsce osiągnięcia korzyści, chyba że Klient dostarczy IBM dodatkowe informacje. Klient odpowiada za aktualizowanie tych informacji i informowanie IBM o każdej ich zmianie.

6.7 Dane normatywne

Bez względu na stanowiące inaczej warunki, IBM ma prawo przechowywać i wykorzystywać dane odzwierciedlające indywidualny sposób korzystania przez autoryzowanych użytkowników Klienta z usługi IBM SaaS w postaci zbiorczej i anonimowej (tzn. w postaci, która uniemożliwia zidentyfikowanie Klienta i jego autoryzowanych użytkowników jako źródła danych, oraz z pominięciem wszelkich informacji umożliwiających identyfikację osobistą), przy czym dane te będą przechowywane i używane wyłącznie do prowadzenia badań i analiz normatywnych, przygotowywania demonstracji oraz raportowani.

6.8 Legalne używanie i wyrażenie zgody

6.8.1 Zgoda na gromadzenie i przetwarzanie danych

Usługa IBM SaaS jest przeznaczona do zarządzania urządzeniami mobilnymi, udostępniania ich, zabezpieczania, monitorowania i nadzorowania. Usługa gromadzi dane użytkowników i urządzeń upoważnionych przez Klienta do korzystania z zasubskrybowanej przez niego usługi IBM SaaS. Usługa IBM SaaS gromadzi informacje, które osobno lub w określonym połączeniu mogą być uznane za dane osobowe według ustawodawstwa niektórych krajów. Gromadzone dane mogą obejmować imię i nazwisko autoryzowanego użytkownika, jego zarejestrowany adres e-mail i lokalizację urządzenia, identyfikator użytkownika i historię bezpiecznego przeglądania, informacje o sprzęcie, oprogramowaniu i ustawieniach użytkownika końcowego, a także informacje generowane przez urządzenie. Klient upoważnia IBM do gromadzenia, przetwarzania i używania tych informacji zgodnie z niniejszymi Warunkami Używania.

6.8.2 Świadoma zgoda właścicieli danych

Korzystanie z 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 zgadza 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.

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 jako administratorowi danych Klienta za pośrednictwem usługi IBM SaaS. Klient niniejszym 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 adresem <http://www.ibm.com/software/sla/sladb.nsf/>.

6.9 Przechowywanie danych

IBM usunie wszelkie zgromadzone informacje, które mogą zawierać Dane Osobowe, po rozwiązaniu niniejszych Warunków Używania, z wyłączeniem informacji, które IBM ma obowiązek przechowywać w celach określonych powyżej albo zgodnie z obowiązującym prawem lub regulacjami. W przypadku takich informacji IBM będzie je przechowywać przez okres wskazany w odnośnym przepisie lub uregulowaniu albo w opisie wskazanego celu.

Dodatek A

MobileFirst Protect to łatwa w obsłudze platforma przetwarzania w chmurze, która udostępnia wszystkie podstawowe funkcje niezbędne do kompleksowego zarządzania nowoczesnymi urządzeniami mobilnymi, takimi jak iPhone'y, iPady, urządzenia Kindle Fire, smartfony Blackberry, telefony z systemem Windows oraz urządzenia z systemem Android. Poniżej podano krótki opis oferty tych usług IBM SaaS:

1. IBM MobileFirst Protect – Devices (SaaS)

Podstawowe funkcje MDM (zarządzania urządzeniami mobilnymi) obejmują: rejestrację urządzeń, konfigurację, zarządzanie strategiami bezpieczeństwa oraz wykonywanie działań w odniesieniu do urządzenia, takich jak wysyłanie wiadomości, lokalizowanie, blokowanie i czyszczenie. Zaawansowane funkcje MDM oferują między innymi zautomatyzowane zarządzanie regułami zgodności, ustawienia prywatności w modelu BYOD (w którym pracownicy korzystają z prywatnych urządzeń w kontekście służbowym), a także panele kontrolne i raporty umożliwiające analizę danych o urządzeniach mobilnych.

2. IBM MobileFirst Protect – Applications (SaaS)

MobileFirst Protect Applications umożliwia wprowadzanie i dystrybucję aplikacji na obsługiwane urządzenia, zarządzane za pomocą programu MobileFirst Protect. W skład tej oferty wchodzi MobileFirst Protect App Catalog, aplikacja instalowana na urządzeniu, za pomocą której użytkownicy mogą wyświetlać i instalować aplikacje zarządzane, a także otrzymywać powiadomienia o ich aktualizacjach.

3. IBM MobileFirst Protect – Application Security (SaaS)

MobileFirst Protect Application Security zapewnia dodatkową ochronę danych w aplikacjach korporacyjnych, które podczas programowania korzystają z pakietu WorkPlace SDK, a w przypadku aplikacji iOS umożliwia także automatyczną integrację certyfikatu podpisu, łatwe przesyłanie pliku aplikacji (.ipa) oraz powiązanie z nim profilu udostępniania. Rozwiązanie Mobile Application Security integruje aplikację z pakietem Secure Productivity Suite. Umożliwia to pojedyncze logowanie, dostęp do intranetu za pośrednictwem bramy Mobile Enterprise Gateway, a także egzekwowanie ustawień ochrony danych.

4. IBM MobileFirst Protect – Gateway for Apps (SaaS)

MobileFirst Protect Gateway for Apps zapewnia użytkownikom przebywającym poza siecią korporacyjną bezpieczny, bezproblemowy dostęp do wewnętrznych zasobów aplikacji bez potrzeby stosowania pełnego połączenia VPN na urządzeniu.

5. IBM MobileFirst Protect – Content (SaaS)

MobileFirst Protect Content umożliwia administratorom wprowadzanie i dystrybucję dokumentów na obsługiwane urządzenia, zarządzane za pomocą programu IBM MobileFirst Protect Devices. W skład tego rozwiązania wchodzi IBM MobileFirst Protect Doc Catalogue, instalowany na urządzeniu, chroniony hasłem kontener, który umożliwia użytkownikom uzyskiwanie bezpiecznego i łatwego dostępu do dokumentów oraz ich wyświetlanie i udostępnianie do współużytkowania. Co więcej, rozwiązanie zapewnia bezproblemowy dostęp do zawartości rozproszonej i repozytoriów takich jak SharePoint, Box i Google Drive. Dostęp do prywatnych współużytkowanych zasobów plikowych SharePoint i plików udostępnionych w systemie Windows jest realizowany za pośrednictwem bramy MobileFirst Protect Mobile Enterprise Gateway. W ramach zarządzania dokumentami za pomocą usługi MobileFirst Protect można stosować kontrolę wersji, poddawać dokumenty audytowi i chronić je przed utratą danych za pomocą opcji strategii DLP (Data Loss Prevention). Opcje te mogą obejmować obowiązek uwierzytelniania, ograniczenie możliwości kopiowania i wklejania oraz blokowanie dokumentu przed otwarciem lub udostępnieniem w innych aplikacjach.

6. IBM MobileFirst Protect – Document Sync (SaaS)

MobileFirst Protect Document Sync umożliwia łatwe i bezpieczne synchronizowanie zawartości użytkowników na zarządzanych urządzeniach mobilnych. Dzięki temu administratorzy mogą zagwarantować, że strategie ochrony zawartości użytkownika, np. ograniczenia możliwości wycinania, kopiowania i wklejania oraz blokada otwierania lub udostępniania zawartości w innych aplikacjach, zostały wdrożone na wszystkich urządzeniach. Zawartość jest przechowywana w bezpieczny sposób

zarówno w chmurze, jak i na urządzeniu, a dostęp do niej można uzyskać tylko za pośrednictwem aplikacji MobileFirst Protect Doc Catalogue.

7. IBM MobileFirst Protect – Document Editor (SaaS)

MobileFirst Protect Document Editor to pakiet biurowy o ogromnych możliwościach, który umożliwia pracę nad dokumentami służbowymi na urządzeniach mobilnych, oferując następujące funkcje:

- tworzenie i edytowanie plików .DOC, .PPT oraz .XLS;
- korzystanie z trybu prezentacji slajdów;
- wygodną pracę z załącznikami do wiadomości e-mail i innymi plikami za pomocą rozwiązania MobileFirst Protect for iOS.

8. IBM MobileFirst Protect – Gateway for Documents (SaaS)

Usługa MobileFirst Protect Gateway for Documents umożliwia wykorzystanie rozwiązania MobileFirst Protect Content w celu zaoferowania dodatkowego, bezpiecznego i bezproblemowego dostępu urządzeń poza siecią korporacyjną do wewnętrznych serwisów Connections i SharePoint, udostępnionych plików Windows i innych składnic plików bez potrzeby stosowania pełnej konfiguracji VPN na urządzeniu. W celu korzystania z usługi MobileFirst Protect Gateway for Documents należy również nabyć rozwiązanie MobileFirst Protect Content. Obsługiwane systemy operacyjne to iOS 5.0 oraz Android 4.0 lub nowsze.

9. IBM MobileFirst Protect – Email Management (SaaS)

Usługa MobileFirst Protect Email Management udostępnia kluczowe funkcje obsługi rozwiązań Microsoft Exchange ActiveSync oraz Lotus Traveler.

- Exchange ActiveSync: zapewnia obsługę urządzeń mobilnych łączących się z serwerem Microsoft Exchange za pośrednictwem protokołu ActiveSync. Oferowane możliwości obejmują podstawowe funkcje zarządzania urządzeniem mobilnym, takie jak możliwość konfigurowania urządzeń, tworzenia i wdrażania strategii ActiveSync (hasło, blokada lub zezwolenie na dostęp do poczty elektronicznej), a także wykonywanie działań na urządzeniu, takich jak blokowanie i czyszczenie oraz generowanie szczegółowych raportów o atrybutach urządzenia.
- Lotus Traveler: obsługa urządzeń mobilnych łączących się z produktem IBM Lotus Notes® za pośrednictwem protokołu Lotus Traveler. Oferowane funkcje obejmują możliwość konfigurowania urządzeń, ich blokowania lub dopuszczania, egzekwowania strategii haseł, czyszczenia urządzeń oraz generowania szczegółowych raportów o atrybutach urządzeń.

10. IBM MobileFirst Protect – Browser (SaaS)

MobileFirst Protect Browser to wszechstronna przeglądarka WWW, umożliwiająca uzyskanie bezpiecznego dostępu do korporacyjnego intranetu oraz zapewniająca zgodność ze strategiami dotyczącymi zawartości. Jest to możliwe dzięki filtrowaniu serwisów WWW i wdrażaniu strategii bezpieczeństwa gwarantujących, że użytkownicy uzyskują dostęp tylko do zatwierdzonej zawartości WWW. Zawartość taką można definiować na podstawie szeregu różnych kategorii, takich jak serwisy społecznościowe, treści dla dorosłych albo serwisy zawierające szkodliwe oprogramowanie. Można również wyłączać wbudowane przeglądarki WWW urządzenia albo przeglądarki WWW innych producentów, stosując strategię aplikacji lub listy zablokowanych obiektów („czarne listy”) w połączeniu z rozwiązaniem MobileFirst Protect Devices. Zakres możliwości obejmuje ponadto tworzenie list wyjątków („białych list”) serwisów WWW, ograniczania plików cookie, zarządzanie obsługą funkcji kopiowania, wklejania i drukowania oraz włączanie trybu Kiosk.

11. IBM MobileFirst Protect – Gateway for Browser (SaaS)

MobileFirst Protect Gateway for Browser umożliwia uzyskiwanie dostępu z obsługiwanego urządzenia do zatwierdzonych wewnętrznych serwisów WWW bez potrzeby stosowania pełnej konfiguracji połączenia VPN na urządzeniu.

12. IBM MobileFirst Protect for Blackberry (SaaS)

Zapewnia obsługę urządzeń połączonych z serwerem BlackBerry Enterprise Server (BES) z wykorzystaniem interfejsów API BlackBerry. Zakres możliwości obejmuje wykonywanie zadań zdalnych, takich jak wysyłanie wiadomości, resetowanie hasła, przypisywanie strategii BES oraz czyszczenie urządzenia, a także szczegółowe raporty o atrybutach urządzeń. Niezbędne jest zainstalowanie rozwiązania MobileFirst Protect Cloud Extender. Produkt dostępny tylko dla urządzeń wyświetlanych lub zarządzanych za pomocą programu MobileFirst Protect za pośrednictwem serwera BES 5.0.

13. IBM MobileFirst Protect – Expenses (SaaS)

MobileFirst Protect Expenses umożliwia administratorom tworzenie zasad wykorzystania danych i przypisywanie ich do obsługiwanych urządzeń, zarządzanych za pomocą programu MobileFirst Protect. Zasady można przypisywać na poziomie urządzenia lub grupy albo na poziomie globalnym. Można również konfigurować progi alertów i przesyłanie wiadomości na potrzeby używania danych zarówno we własnej sieci, jak i w roamingu.

14. IBM MobileFirst Protect – Management Suite (SaaS)

Pakiet produktów obejmujący rozwiązania MobileFirst Protect Devices, MobileFirst Protect Applications, MobileFirst Protect Content oraz MobileFirst Protect Expenses.

15. IBM MobileFirst Protect – Productivity Suite (SaaS)

Pakiet produktów obejmujący rozwiązania MobileFirst Protect Secure Mail, MobileFirst Protect Applications, MobileFirst Protect Application Security, MobileFirst Protect Content oraz MobileFirst Protect Browser.

16. IBM MobileFirst Protect – Secure Mail (SaaS)

MobileFirst Protect Secure Mail to odrębna, bezpieczna aplikacja biurowa, umożliwiająca użytkownikom uzyskiwanie dostępu do poczty elektronicznej, kalendarza i danych kontaktowych oraz zarządzanie nimi. Można w niej wdrażać kontrolę wiadomości e-mail i załączników w celu zapobiegania wyciekaniu danych poprzez ograniczenie możliwości przesyłania lub przenoszenia zawartości do innych aplikacji. Ponadto można wymuszać uwierzytelnianie, ograniczać możliwość wycinania, kopiowania i wklejania, a także blokować załączniki e-mail w taki sposób, aby możliwe było tylko ich wyświetlanie.

17. IBM MobileFirst Protect – Gateway Suite (SaaS)

MobileFirst Protect Gateway Suite zapewnia bezpieczną i bezproblemową komunikację obsługiwanych aplikacji w systemach iOS i Android z zasobami w wewnętrznej sieci przedsiębiorstwa.

18. IBM MobileFirst Protect – Content Suite (SaaS)

Pakiet produktów obejmujący rozwiązania MobileFirst Protect Content, MobileFirst Protect Document Editor oraz MobileFirst Protect Document Sync.

19. IBM MobileFirst Protect – Threat Management (SaaS)

MobileFirst Protect Threat Management oferuje rozszerzone funkcje zabezpieczeń urządzeń mobilnych, obejmujące wykrywanie szkodliwego oprogramowania i zaawansowanych technik typu jailbreak/root. Dzięki rozwiązaniu MobileFirst Protect Threat Management Klient może skonfigurować i obsługiwać strategię zgodności w odniesieniu do wykrytego szkodliwego oprogramowania i innych słabych punktów zabezpieczeń.

20. IBM MobileFirst Protect – Content Service (SaaS)

MobileFirst Protect Content Service (SaaS) umożliwia użytkownikom przesyłanie pakietów aplikacji i dokumentów do systemu dystrybucji treści MobileFirst Protect.

Klienci korzystający z usługi MobileFirst Protect Content Service muszą również nabyć co najmniej po jednym uprawnieniu do usługi MobileFirst Protect Content Service Storage (SaaS) oraz do usługi MobileFirst Protect Content Service Bandwidth (SaaS).

21. IBM MobileFirst Protect – Content Service Storage (SaaS)

MobileFirst Protect Content Service Storage (SaaS) umożliwia użytkownikom wykupienie określonej, łącznej ilości pamięci masowej na dane, używanej w połączeniu z usługą MobileFirst Protect Content Service (SaaS).

22. IBM MobileFirst Protect – Content Service Bandwidth (SaaS)

MobileFirst Protect Content Service Bandwidth (SaaS) umożliwia użytkownikom wykupienie określonej, łącznej szerokości pasma używanej w połączeniu z usługą MobileFirst Protect Content Service (SaaS).

23. IBM MobileFirst Protect – Professional (SaaS)

Jest to usługa przeznaczona dla małych i średnich przedsiębiorstw, która zapewnia szybką i prostą metodę zdalnej konfiguracji smartfonów i tabletów, wdrażania strategii bezpieczeństwa, przesyłania aplikacji i dokumentów oraz ochrony danych na urządzeniach firmowych i prywatnych. Dzięki temu

przedsiębiorstwo zyskuje dostęp do niezbędnych funkcji zarządzania środowiskiem mobilnym — łatwo, szybko i w przystępnej cenie.

24. IBM MobileFirst Protect – Laptop (SaaS)

Jest to usługa umożliwiająca Klientom obsługę urządzeń, w tym komputerów z systemami OS X i Windows oraz smartfonów i tabletów, obejmującą czynności związane z ich rejestrowaniem, konfigurowaniem i zabezpieczaniem, zarządzaniem nimi i generowaniem raportów. Pozwala to przedsiębiorstwom utrzymać spójność strategii i profili bezpieczeństwa na urządzeniach należących do firmy i na prywatnych urządzeniach pracowników, którymi zarządza się z jednej konsoli MobileFirst Protect.

24.1 Windows

MobileFirst Protect – Laptop (SaaS) dla komputerów osobistych z systemem Windows umożliwia bezprzewodowe rejestrowanie urządzeń i generowanie raportów dotyczących zarządzania zasobami obejmującymi sprzęt, system operacyjny i oprogramowanie. Moduł raportowania bezpieczeństwa punktów końcowych przekazuje interaktywne raporty i analizy danych dla aplikacji dostarczonych przez Klienta, takich jak programy antywirusowe, systemy tworzenia i odtwarzania kopii zapasowych, narzędzia do szyfrowania danych i osobisty firewall, a także zgłasza braki w poprawkach do systemu operacyjnego. Moduł ochrony danych przedstawia interaktywne raporty i analizy dotyczące usług bezpieczeństwa, obejmujących szyfrowanie danych, zapobieganie wyciekom danych, tworzenie i odtwarzanie kopii zapasowych oraz inne aplikacje zintegrowane. Obsługiwane są systemy operacyjne Windows XP SP3, Windows Vista, Windows 7, Windows 8+ i Windows 8+ Pro (w tym odpowiednio ich edycje 32- i 64-bitowe).

Dostępne są następujące działania w odniesieniu do urządzeń:

- wysyłanie wiadomości na urządzenie;
- blokowanie urządzenia;
- określanie lokalizacji urządzenia (wymagana jest usługa MobileFirst Protect Laptop Location);
- zatrzymywanie, uruchamianie i restartowanie usług;
- zamykanie i ponowne uruchamianie;
- usuwanie danych z dysku twardego;
- konfigurowanie ustawień poprawek;
- dystrybuowanie oprogramowania.

24.2 Mac OS X

MobileFirst Protect – Laptop (SaaS) dla komputerów z systemem Mac OS X umożliwia bezprzewodowe rejestrowanie urządzeń i generowanie raportów dotyczących zarządzania zasobami obejmującymi sprzęt, system operacyjny i oprogramowanie. Moduł raportowania bezpieczeństwa punktów końcowych przekazuje interaktywne raporty i analizy danych dla aplikacji dostarczonych przez Klienta, takich jak programy antywirusowe, systemy tworzenia i odtwarzania kopii zapasowych, narzędzia do szyfrowania danych i osobisty firewall, a także zgłasza braki w poprawkach do systemu operacyjnego. Moduł ochrony danych przedstawia interaktywne raporty i analizy dotyczące usług bezpieczeństwa, obejmujących szyfrowanie danych. Moduł zarządzania konfiguracją umożliwia zdalne zarządzanie wieloma ustawieniami urządzeń i użytkowników, takimi jak hasła, adresy e-mail, sieć VPN i połączenia Wi-Fi. Obsługiwany jest system operacyjny Mac OS X w wersji 10.7.3 lub nowszej.

Dostępne są następujące działania w odniesieniu do urządzeń:

- blokowanie urządzenia;
- usuwanie danych z dysku twardego;
- zmiana strategii urządzenia.

25. IBM MobileFirst Protect – Laptop Location (SaaS)

Usługa MobileFirst Protect Laptop Location (SaaS) umożliwia określanie lokalizacji obsługiwanych laptopów i tabletów. MobileFirst Protect zgłasza współrzędne określające lokalizację adresu Wi-Fi lub IP i przekształca te informacje do łatwo zrozumiałej postaci. Gdy urządzenie jest włączone, można sprawdzić jego aktualne położenie. MobileFirst Protect przechowuje zgłaszane dane o położeniu, co umożliwia późniejsze przeglądanie historii lokalizacji. Do korzystania z tej usługi wymagane jest rozwiązanie IBM

MobileFirst Protect Laptop (SaaS) for Windows. Obsługiwane są systemy operacyjne Windows XP SP3, Windows Vista, Windows 7, Windows 8+ i Windows 8+ Pro (w tym odpowiednio ich edycje 32- i 64-bitowe).

26. IBM MobileFirst Protect – Laptop Lifecycle Management (SaaS)

Usługa ta oferuje funkcje dostępne w rozwiązaniu MobileFirst Protect – Laptop (SaaS), uzupełnione o następujące możliwości:

- Funkcję przesyłania pakietów do platformy MobileFirst Protect Content Service (SaaS) i planowania harmonogramu dystrybucji zawartości na urządzenia zarządzane za pośrednictwem usługi MobileFirst Protect Laptop (SaaS) dla systemu Microsoft Windows. Klient może sterować wszystkimi aspektami dystrybucji, w tym instrukcjami instalowania i wyborem odbiorców na poziomie urządzenia lub grupy albo na poziomie globalnym. Klient odpowiada za przygotowanie pakietów i plików instalacyjnych. IBM nie udziela wsparcia w zakresie tworzenia pakietów instalacyjnych.

27. IBM MobileFirst Protect – Laptop Security and Compliance (SaaS)

Usługa ta pozwala przedsiębiorstwom na utrzymywanie spójności strategii i profili bezpieczeństwa na urządzeniach należących do firmy i na prywatnych urządzeniach pracowników, którymi zarządza się z jednej konsoli.

28. IBM MaaS360 Advanced Mobile Management Suite Prime (SaaS)

Podstawowe funkcje MDM (zarządzania urządzeniami mobilnymi) obejmują: rejestrację urządzeń, konfigurację, zarządzanie strategiami bezpieczeństwa oraz wykonywanie działań w odniesieniu do urządzenia, takich jak wysyłanie wiadomości, lokalizowanie, blokowanie i czyszczenie. Zaawansowane funkcje MDM oferują między innymi zautomatyzowane zarządzanie regułami zgodności, ustawienia prywatności w modelu BYOD (w którym pracownicy korzystają z prywatnych urządzeń w kontekście służbowym), a także panele kontrolne i raporty umożliwiające analizę danych o urządzeniach mobilnych.

29. IBM MaaS360 Secure Productivity Suite Prime (SaaS)

Ta usługa umożliwia uzyskiwanie bezpiecznego dostępu do poczty elektronicznej, przechowywanie i dystrybucję aplikacji oraz zarządzanie nimi, a także uzyskiwanie dostępu do serwisu intranetowego przy użyciu bezpiecznej przeglądarki.

30. IBM MaaS360 Secure Document Sharing Suite Prime (SaaS)

Ta usługa umożliwia zdalne zarządzanie smartfonami i tabletami, konfigurowanie ich, egzekwowanie strategii bezpieczeństwa, dystrybuowanie danych, sporządzanie raportów z używania połączeń Wi-Fi w celu śledzenia poziomu wykorzystania transmisji danych i ponoszonych wydatków, a także przechowywanie zawartości i dystrybuowanie aplikacji i dokumentów.

31. IBM MaaS360 Professional Bundle Prime (SaaS)

Jest to usługa, która umożliwia małym i średnim przedsiębiorstwom zdalne konfigurowanie smartfonów i tabletów, wdrażanie strategii bezpieczeństwa, przesyłanie aplikacji i dokumentów oraz ochronę danych na urządzeniach firmowych i prywatnych.

32. IBM MaaS360 Educational Bundle Prime (SaaS)

Ta usługa umożliwia instytucjom edukacyjnym zdalne zarządzanie smartfonami i tabletami oraz konfigurowanie ich, egzekwowanie strategii bezpieczeństwa, dystrybuowanie danych, dystrybuowanie aplikacji, przechowywanie ich zawartości oraz zarządzanie nimi.

33. IBM MaaS360 Advanced Laptop Management Prime (SaaS)

Ta usługa umożliwia zarządzanie oprogramowaniem na laptopach oraz jego aktualizowanie, dystrybuowanie i lokalizowanie, co umożliwia wprowadzenie spójnych strategii bezpieczeństwa na wszystkich komputerach typu laptop i desktop, które komunikują się z konsolą administracyjną MaaS360.

Warunki Używania Produktów i Usług IBM — zobowiązania dotyczące poziomu usług

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 Proof of Entitlement (PoE) lub w Dokumencie Transakcyjnym Klienta.

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** — Przestój Aplikacji i/lub Przestój Przetwarzania Przychodzących Danych dotyczący Poziomu Usług podanego w poniższej tabeli. Za Przestój nie uznaje się okresu, w którym usługa IBM SaaS 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 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 Przeszojów w każdym Miesiącu Obowiązywania Umowy w odniesieniu do stosownego Poziomu Usług wskazanego w poniższej tabeli. Uznania z tytułu Dostępności będą zależeć od czasu trwania Przeszojów mierzonego od daty i godziny zgłoszonego pierwszego wystąpienia Przeszoju. Jeśli Klient zgłosi jednocześnie Zdarzenie Przeszoju Aplikacji oraz Zdarzenie Przeszoju Przetwarzania Danych Przychodzących, IBM potraktuje nakładające się okresy Przeszoju jako jeden i ten sam okres Przeszoju, a nie jako dwa oddzielne okresy Przeszoju. 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)
Mniej niż 99,8%	2%
Mniej niż 98,8%	5%
Mniej niż 95,0%	10%

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

Przykład: łączny czas trwania Przeszojów w Miesiącu Obowiązywania Umowy = 50 minut

43 200 minut w 30-dniowym Miesiącu Obowiązywania Umowy - 50 minut Przeszoju = 43 150 minut <hr/> łącznie 43 200 minut	= 2% Uznanie z tytułu Osiągniętego Poziomu Usług na poziomie 99,8% w Miesiącu Obowiązywania Umowy
---	---

4. 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 też zatwierdzonych gości Klienta IBM korzystających z usługi IBM SaaS;
- Oprogramowania Pomocniczego.