Podmienky používania IBM – Podmienky pre konkrétnu ponuku služieb SaaS

IBM Security Trusteer Fraud Protection

Podmienky používania pozostávajú z tohto dokumentu Podmienky používania IBM – Podmienky pre konkrétnu ponuku služieb SaaS („Podmienky pre konkrétnu ponuku služieb SaaS“) a dokumentu s názvom Podmienky používania IBM – Všeobecné podmienky („Všeobecné podmienky“), ktorý je k dispozícii na adrese: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V prípade nesúladu medzi Podmienkami pre konkrétnu ponuku služieb SaaS a Všeobecnými podmienkami sa budú uplatňovať ustanovenia Všeobecných podmienok. Objednaním služby IBM SaaS, prístupom k nej a jej používaním Zákazník vyjadruje súhlas s týmito Podmienkami používania.

Tieto Podmienky používania sa riadia zmluvou IBM International Passport Advantage Agreement alebo zmluvou IBM International Passport Advantage Express Agreement alebo IBM International Agreement for Selected IBM SaaS Offerings, podľa toho, ktorá sa uplatňuje, (ďalej len „Zmluva“) a spoločne s Podmienkami používania tvoria úplnú zmluvu.

1. IBM SaaS

Podmienky pre konkrétnu ponuku služieb SaaS sa vzťahujú na nasledujúce ponuky IBM SaaS:

1.1 Ponuky 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 Ponuky 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 Ponuky Mobile IBM SaaS

- 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. Platobné metriky

Služba IBM SaaS sa poskytuje na základe nasledujúcich účtovných metrík špecifikovaných v Transakčnom dokumente:

a. **Oprávnený účastník** – je merná jednotka, na základe ktorej je možné zakúpiť si službu IBM SaaS. Za Oprávneného účastníka sa považuje každý jednotlivec alebo právna entita, ktorá je oprávnená zúčastňovať sa programu poskytovania služieb spravovaného alebo sledovaného službou IBM SaaS. Zákazník musí zakúpiť dostatočný počet oprávnení, ktorý bude pokrývať všetkých Oprávnených účastníkov riadených alebo sledovaných v službe IBM SaaS počas obdobia merania určeného v Transakčnom dokumente Zákazníka.

   Každý program poskyovania služieb riadený službou IBM SaaS sa analyzuje samostatne a potom sa pridá k ostatným. Jednotlivci alebo entity s oprávnením pre viaceré programy poskytovania služieb si vyžadujú osobitné oprávnenia.

   Program poskytovania služieb pre tieto ponuky zahŕňa jednu Podnikovú alebo Maloobchodnú aplikáciu Zákazníka s hlavnou prihlasovacou stránkou a súvisiacimi stránkami pre každú Podnikovú alebo Maloobchodnú aplikáciu. Oprávnený účastník je koncový užívateľ Zákazníka, ktorý má prihlasovacie údaje do Podnikovej alebo Maloobchodnej aplikácie.

b. **Klientske zariadenie** – je merná jednotka, na základe ktorej je možné zakúpiť službu IBM SaaS. Klientske zariadenie je výpočtové zriadenie pre jedného užívateľa alebo senzor osobitného účelu alebo telemetrické zariadenie, ktoré požaduje vykonanie alebo pre vykonanie prijíma sadu príkazov, procedúr alebo aplikácií od alebo poskytuje údaje inému výpočtovému systému, ktorý sa zvyčajne označuje ako server alebo ho server spravuje. Viaceré Klientske zariadenia môžu zdieľať prístup k spoločnému serveru. Klientske zariadenie môže mať určitú schopnosť spracovania alebo je ho možné naprogramovať, aby umožnilo prácu užívateľa. Zákazník musí zakúpiť oprávnenia pre každé Klientske zariadenie, ktoré sa používa, poskytuje údaje, používa poskytované služby alebo inak pristupuje k službe IBM SaaS počas obdobia merania uvedeného v Transakčnom dokumente Zákazníka.

3. Poplatky a fakturácia

Suma splatná za službu IBM SaaS je uvedená v Transakčnom dokumente.

3.1 Čiastkové mesačné poplatky

Čiastkové mesačné poplatky, ako sú definované v Transakčnom dokumente, sa môžu účtovať pomerne.

4. Súlad s nariadeniami a audit

Prístup k ponukám IBM Security Trusteer Fraud Protection podlieha maximálnemu množstvu Oprávnených účastníkov alebo Klientskych zariadení, ktorý je uvedený v Transakčnom dokumente. Zákazník je povinný zabezpečiť, aby počet Oprávnených účastníkov alebo Klientskych zariadení nepresiahol maximálne množstvo, ktoré je uvedené v Transakčnom dokumente.

Audit sa môže vykonať kvôli overeniu súladu s nariadením maximálneho množstva Oprávnených účastníkov alebo Klientskych zariadení.

5. Voľby obnovenia Doby predplatného IBM SaaS

To, či sa služba IBM SaaS obnoví na konci Doby predplatného, bude určené v Transakčnom dokumente Zákazníka, a to prostredníctvom niektorej z nasledujúcich možností:

5.1 Automatické obnovenie

Ak je v Transakčnom dokumente Zákazníka uvedené, že obnovenie služieb je automatické, Zákazník môže ukončiť aktuálnu Dobu predplatného služby IBM SaaS poskytnutím písomnej výpovede obchodnému zástupcovi spoločnosti IBM alebo obchodnému partnerovi spoločnosti IBM najneskôr deväťdesiat (90) dní pred dátumom ukončenia platnosti, ktorý je uvedený v Transakčnom dokumente. Ak IBM alebo jej IBM Business Partner nedostane takéto oznámenie o ukončení do dátumu ukončenia platnosti, končiaca Doba predplatného sa automaticky obnoví buď na jeden rok alebo na rovnaké obdobie aké mala pôvodná Doba predplatného uvedené v Transakčnom dokumente.

5.2 Priebežné vyúčtovanie

Ak je v Transakčnom dokumente uvedené, že zmluva Zákazníka sa bude nepretržite obnovovať, Zákazník bude mať naďalej prístup k službe IBM SaaS a bude sa mu priebežne účtovať používanie služby IBM SaaS. Ak už Zákazník nebude chcieť ďalej používať službu IBM SaaS a bude chcieť zastaviť proces priebežnej fakturácie, musí IBM alebo obchodnému partnerovi IBM doručiť výpoveď najneskôr deväťdesiat (90) dní vopred, v ktorej požiada o zrušenie poskytovania služby IBM SaaS Zákazníkovi. Po zrušení prístupu Zákazníka budú Zákazníkovi fakturované zostávajúce poplatky za prístup počas mesiaca, v ktorom zrušenie nadobudlo platnosť.

5.3 Vyžadované obnovenie

Ak je v Transakčnom dokumente uvedené, že Zákazníkov typ obnovenia zmluvy je „ukončiť“, poskytovanie služby IBM SaaS sa na konci Doby predplatného ukončí a prístup Zákazníka k službe IBM SaaS bude odstránený. Ak bude chcieť Zákazník pokračovať v používaní služby IBM SaaS aj po dátume ukončenia, Zákazník si musí u Zákazníkovho obchodného zástupcu IBM alebo u Obchodného partnera IBM objednať nákup novej Doby predplatného.

6. Technická podpora

Zákazníkovi a jeho Oprávneným účastníkom sa bude poskytovať technická podpora pre službu IBM SaaS s cieľom pomôcť im pri používaní služby IBM SaaS.

Štandardná podpora je súčasťou predplatného všetkých ponúk. Služba Trusteer Rapport Mandatory Service, ktorá je prídavným komponentom pre Trusteer Rapport, má nevyhnutnú podmienku podpory Premium Support pre základné predplatné Trusteer Rapport.

Pre každú ponuku IBM SaaS je predplatné podpory Premium Support k dispozícii za príplatok, s výnimkou ponúk IBM Security Trusteer Mobile SDK a ponúk IBM Security Trusteer Rapport Mandatory Service.

Štandardná podpora:

- Podpora od 8. do 17. miestneho času.
- Zákazníci a Oprávnení účastníci môžu žiadosti o podporu posielať elektronicky, ako je uvedené v Príručke podpory pre službu SaaS (Software as a Service).
- Oznamy, dokumenty, hlásenia prípadov a najčastejšie otázky môžu Zákazníci nájsť na Portáli zákazníckej podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Voľby a podrobnosti podpory nájdete v Príručke podpory pre IBM SaaS (Software as a Service) na adrese: http://www-01.ibm.com/software/support/handbook.html.

Premium Support:

- Nepretržitá podpora pre všetky závažnosti problémov.

- Zákazníci môžu kontaktovať podporu priamo prostredníctvom telefónu.
- Zákazníci a Oprávnení účastníci môžu žiadosti o podporu posielať elektronicky, ako je uvedené v Príručke podpory pre službu SaaS (Software as a Service).
- Oznamy, dokumenty, hlásenia prípadov a najčastejšie otázky môžu Zákazníci nájsť na Portáli zákazníckej podpory na adrese: http://www-01.ibm.com/software/security/trusteer/support/.
- Voľby a podrobnosti podpory nájdete v Príručke podpory pre IBM SaaS (Software as a Service) na adrese: http://www-01.ibm.com/software/support/handbook.html.

7. Ďalšie podmienky vzťahujúce sa na ponuku IBM SaaS

7.1 Súlad s programom Bezpečný prístav

IBM dodržuje program Bezpečný prístav medzi USA a EÚ vytvorený Ministerstvom obchodu USA v spolupráci Európskou komisiou. Produkty IBM Security Trusteer sú súčasťou certifikácie v programe Bezpečný prístav medzi USA a EÚ udelenej spoločnosti IBM. Ďalšie informácie o programe Bezpečný prístav a zoznam spoločností certifikovaných v programe Bezpečný prístav je k dispozícii na adrese: http://export.gov/safeharbor/.

7.2 Navýšenie poplatku Ročného predplatného

IBM si vyhradzuje právo upravovať poplatok za predplatné IBM SaaS maximálne raz za dvanásť (12) mesiacov o percento, ktoré stanoví IBM a ktoré neprekročí 3%. Úprava poplatku za predplatné nadobudne účinnosť v deň výročia prvého začiatočného obdobia pokrytia. Táto úprava poplatku nemení oprávnenie Zákazníka pre službu IBM SaaS ani metriku spoplatňovania, na základe ktorej si zakúpil službu IBM SaaS. IBM Business Partneri sú nezávislí od IBM a svoje ceny a podmienky stanovujú samostatne.

7.3 Premium Support

Zákazník má nárok na podporu Premium Support len pri ponukách IBM SaaS, pri ktorých si Zákazník predplatil súvisiacu ponuku Premium Support.

7.4 Legálne používanie a súhlas

Oprávnenie na zhromažďovanie a spracovanie údajov

Táto služba IBM SaaS je navrhnutá tak, aby pomáhala Zákazníkovi zlepšiť bezpečnosť prostredia a údajov. Služba IBM SaaS bude zhromažďovať informácie od Oprávnených účastníkov a z Klientskych zariadení, ktoré interaktívne pracujú s Podnikovými alebo Maloobchodnými aplikáciami, pri ktoré si Zákazník predplatil službu IBM SaaS. IBM SaaS zhromažďuje informácie, ktoré môžu byť v niektorých oblastiach samostatne alebo spoločne považované za Osobné informácie. Osobné údaje sú ľubovoľné informácie, na základe ktorých je možné identifikovať konkrétneho jednotlivca, ako sú meno, e-mailová adresa, domáca adresa alebo telefónne číslo, a ktoré sa poskytnú IBM za účelom ich uloženia, spracovania alebo prenosu v mene Zákazníka.

Postupy zhromažďovania a spracovania údajov sa môžu aktualizovať kvôli zlepšeniu funkčnosti IBM SaaS. Dokument s úplným popisom postupov zhromažďovania a spracovania údajov sa podľa potreby aktualizuje a na požiadanie bude poskytnutý Zákazníkovi. Zákazník oprávňuje IBM, aby zhromažďovala tieto informácie a spracovala ich v súlade s ustanoveniami uvedenými v odsekoch Cezhraničné prevody a Utajenie údajov a zabezpečenie údajov v časti Všeobecné podmienky týchto Podmienok používania.

Pre ponuky IBM Security Trusteer Pinpoint:

Zhromaždené údaje môžu zahŕňať IP adresy užívateľov, šifrované alebo jednosmerne hašované ID užívateľov, objekty cookie domén, ak nie sú filtrované, návštevy chránených Aplikácií a phishingových lokalít a prihlasovacie údaje zadané na phishingových lokalitách.

Pre ponuky IBM Security Trusteer Mobile SDK a ponuky IBM Security Trusteer Mobile Browser:

Zhromaždené údaje môžu zahŕňať IP adresy užívateľov, šifrované alebo jednosmerne hašované ID užívateľov, informácie o geografickej polohe a návštevy chránených Aplikácií, informácie o kartách SIM, názov zariadenia a Zákazníkovu príslušnosť.

Pre ponuky IBM Security Trusteer Rapport:

Zhromaždené údaje môžu zahŕňať IP adresy užívateľov, šifrované alebo jednosmerne hašované ID užívateľov, bezpečnostné udalosti, mená užívateľov a e-mailové adresy poskytnuté na účely kontaktovania zákazníckej podpory IBM, príslušnosť Zákazníka, šifrované heslo zadané v chránených

lokalitách, návštevy chránených Aplikácií a phishingových lokalít, šifrované číslo platobnej karty a súbory a údaje zhromaždené na diaľku pracovníkmi IBM za účelom kontroly podozrivého malvéru, škodlivej činnosti alebo zlyhaní.

Informovaný súhlas zo strany Dátových subjektov:

Používanie tejto IBM SaaS môže zahŕňať dodržiavanie rôznych zákonov alebo predpisov. IBM SaaS sa môže používať len na zákonné účely a zákonným spôsobom. Zákazník súhlasí s tým, že bude službu IBM SaaS používať v súlade s platnými zákonmi, predpismi a smernicami a preberá všetku zodpovednosť za ich dodržiavanie.

Pre ponuky IBM Security Trusteer Pinpoint a IBM Security Trusteer Mobile SDK:

Zákazník prehlasuje, že získal alebo získa všetky plne informované súhlasy, oprávnenia alebo licencie potrebné na umožnenie zákonného používania služby IBM SaaS a že povolí IBM zhromažďovať a spracovávať informácie prostredníctvom služby IBM SaaS.

Pre ponuky IBM Security Trusteer Rapport a pre ponuky & IBM Security Trusteer Mobile Browser:

Zákazník udeľuje IBM oprávnenie na získanie plne informovaných súhlasov potrebných na umožnenie zákonného používania služby IBM SaaS a zhromažďovanie a spracovávanie informácií v súlade s popisom v Licenčnej zmluve koncového užívateľa, ktorá je k dispozícii na adrese https://www.trusteer.com/support/end-user-license-agreement. V prípade, že Zákazník stanoví, že komunikáciu s koncovými užívateľmi v súvislosti s týmito súhlasmi bude zabezpečovať on (a nie IBM), Zákazník prehlasuje, že získal alebo získa všetky plne informované súhlasy, oprávnenia alebo licencie potrebné na umožnenie zákonného používania služby IBM SaaS a že umožní IBM zhromažďovať a spracovávať informácie prostredníctvom služby IBM SaaS z pozície spracovateľa údajov Zákazníka.

7.5 Medzihraničné prevody

Zákazník súhlasí, že IBM môže spracovávať Obsah vrátane všetkých Osobných údajov v zahraničí v súlade s platnými zákonmi a požiadavkami vzťahujúcimi sa na sprostredkovateľov a subdodávateľov v nasledujúcich krajinách mimo Európskeho hospodárskeho priestoru a v krajinách, ktoré Európska komisia považuje za krajiny s dostatočnou úrovňou zabezpečenia: USA.

7.6 Ochrana osobných údajov

Ak Zákazník sprístupní Osobné údaje v službe IBM SaaS v členských štátoch EÚ, na Islande, v Lichtenštajnsku, Nórsku alebo Švajčiarsku, alebo ak má Zákazník Oprávnených účastníkov alebo Klientske zariadenia v uvedených krajinách, potom Zákazník ako výhradný prevádzkovateľ vymenuje IBM ako sprostredkovateľa pre spracovanie (v súlade s definíciou týchto pojmov v Smernici EÚ 95/46/EC) Osobných údajov. IBM spracuje takéto Osobné údaje len v rozsahu nevyhnutnom na sprístupnenie služby IBM SaaS v súlade s popismi služby IBM SaaS zverejnenými IBM a Zákazník súhlasí, že každé takéto spracovanie sa vykoná na základe pokynov Zákazníka. V prípade, že IBM významne zmení miesto spracovania Osobných údajov alebo spôsob ich zabezpečenia v rámci služby IBM SaaS, bude Zákazníka informovať o tejto skutočnosti v dostatočnom predstihu. Zákazník môže vypovedať aktuálnu Dobu predplatného pre príslušnú službu IBM SaaS a to poskytnutím písomnej výpovede IBM do tridsiatich (30) dní odo dňa, kedy IBM oznámi túto zmenu Zákazníkovi. Zákazník súhlasí, že IBM môže spracovať Obsah vrátane všetkých Osobných údajov v zahraničí u nasledujúcich spracovávateľov a subdodávateľov:

Názov Spracovávateľa/subdodávateľa	Rola (Spracovateľ alebo subdodávateľ údajov)	Umiestnenie*
Dodávateľský subjekt IBM	Spracovateľ	Ako je uvedené v Transakčnom dokumente
Amazon Web Services LLC	Subdodávateľ	410 Terry Ave. N Seattle, WA 98109 USA
Connectria Corp.	Subdodávateľ	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 USA
IBM Israel Ltd.	Subdodávateľ	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Názov Spracovávateľa/subdodávateľa	Rola (Spracovateľ alebo subdodávateľ údajov)	Umiestnenie*
IBM Corp	Subdodávateľ	1 New Orchard Rd. Armonk, NY 10504 USA

Zákazník súhlasí s tým, že spoločnosť IBM môže po predchádzajúcom upozornení zmeniť tento zoznam krajín, keď usúdi, že je to nevyhnutné z hľadiska poskytovania služby IBM SaaS.

Zákazník súhlasí, že v prípade služieb poskytovaných prostredníctvom dátového centra v Nemecku, ako bude stanovené v rámci procesu poskytnutia služby, môže IBM spracovať Obsah vrátane všetkých Osobných údajov v zahraničí u nasledujúcich spracovávateľov a subspracovávateľov:

Názov Spracovávateľa/Subspracovávateľa	Rola (Spracovateľ alebo Subspracovateľ údajov)	Umiestnenie*
Dodávateľský subjekt IBM	Spracovateľ	Ako je uvedené v Transakčnom dokumente
Amazon Web Services (Nemecko)	Subdodávateľ	Mníchov, Nemecko
IBM Israel Ltd.	Subdodávateľ	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

Zákazník súhlasí, že v prípade služieb poskytovaných prostredníctvom dátového centra v Japonsku, ako bude stanovené v rámci procesu poskytnutia služby, môže IBM spracovať Obsah vrátane všetkých Osobných údajov v zahraničí u nasledujúcich spracovávateľov a subspracovávateľov:

Názov Spracovávateľa/Subspracovávateľa	Rola (Spracovateľ alebo Subspracovateľ údajov)	Umiestnenie*
Dodávateľský subjekt IBM	Spracovateľ	Ako je uvedené v Transakčnom dokumente
Amazon Web Services (Japonsko)	Subdodávateľ	Tokio, Japonsko
IBM Israel Ltd.	Subdodávateľ	94 Derech Em-Hamoshavot 49527 Petach-Tikva Izrael

* Umiestnenia uvedené v týchto tabuľkách označujú adresu centrály Spracovateľa alebo Subdodávateľa. Dátové centrá sa nachádzajú v tej istej krajine.

Zmluvné strany alebo ich príslušné pridružené spoločnosti môžu uzavrieť samostatné štandardné zmluvy s nezmenenými modelovými ustanoveniami definovanými EÚ z pozície ich príslušných rolí v súlade s rozhodnutím Komisie 2010/87/EÚ, pričom voliteľné ustanovenia sa nebudú uplatňovať. Všetky nezhody alebo pohľadávky vyplývajúce z týchto zmlúv, a to aj v prípade, že vznikli na strane pridružených spoločností, budú zmluvné strany riešiť tak, ako keby vznikli medzi nimi na základe tejto Zmluvy.

Príloha A

1. Ponuky IBM SaaS

IBM ponúka tieto služby ako samostatné služby a ponuky alebo ako dodatkové služby a ponuky. Konkrétne ponuky služieb IBM SaaS, ktoré si Zákazník objednal, sú uvedené v Potvrdení o oprávnení Zákazníka.

1.1 Definície pre Podnikové a Maloobchodné

Produkty IBM Security Trusteer Fraud sú licencované na používanie so špecifickými typmi Aplikácií. Aplikácia je definovaná ako niektorý z nasledujúcich typov: Maloobchodná alebo Podniková. K dispozícii sú samostatné ponuky pre Maloobchodné aplikácie a pre Podnikové aplikácie.

- Maloobchodná aplikácia je definovaná ako aplikácia online bankovníctva, mobilná aplikácia alebo e-commerce aplikácia navrhnutá pre obsluhu spotrebiteľov. Na základe predpisov Zákazníka sa niektoré malé podniky môžu klasifikovať ako spôsobilé pre maloobchodný prístup.
- Podniková aplikácia je definovaná ako aplikácia online bankovníctva, mobilná aplikácia alebo e-commerce aplikácia navrhnutá pre obsluhu podnikových, inštitucionálnych subjektov alebo ich ekvivalentov, alebo každá aplikácia, ktorá nie je zaradená do kategórie Maloobchodná.

1.2 Ponuky základného predplatného IBM SaaS

Podnikové ponuky:

- 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

Maloobchodné ponuky:

- 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

S výnimkou ponúk IBM Security Trusteer Mobile SDK existuje pre každú Podnikovú a Maloobchodnú ponuku pridružený produkt Premium Support, ktorý je k dispozícii za príplatok.

1.3 Dodatkové ponuky predplatného IBM SaaS pre ponuky IBM Security Trusteer Rapport

Dodatkové ponuky dostupné pre IBM Security Trusteer Rapport pre Podnik:

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

Dodatkové ponuky dostupné pre IBM Security Trusteer Rapport pre Maloobchod:

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

S výnimkou prídavných komponentov IBM Security Trusteer Rapport Mandatory Service existuje pre každý Podnikový a Maloobchodný prídavný komponent pre ponuky IBM Security Trusteer Rapport pridružený produkt Premium Support, ktorý je k dispozícii za príplatok.

Predplatné pre IBM Security Trusteer Rapport for Business alebo pre IBM Security Trusteer Rapport for Retail je nevyhnutná podmienka pre priradené dodatkové ponuky predplatného pre IBM SaaS, ktoré sú uvedené v tejto časti.

1.4 Dodatkové ponuky predplatného IBM SaaS pre ponuky IBM Security Trusteer Pinpoint Malware Detection

Dodatkové ponuky dostupné pre IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition alebo pre IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Dodatkové ponuky dostupné pre IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition alebo pre 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

Predplatné Premium Support je k dispozícii za príplatok pre všetky dodatkové ponuky IBM SaaS, uvedené v tejto časti.

Predplatné pre ponuky IBM Security Trusteer Pinpoint Malware Detection for Business alebo pre ponuky IBM Security Trusteer Pinpoint Malware Detection for Retail je nevyhnutnou podmienkou pre pridružené dodatkové ponuky predplatného IBM SaaS, ktoré sú uvedené v tejto časti.

1.5 Ostatné dodatkové predplatné pre IBM SaaS

Každé dodatkové predplatné IBM SaaS nad rámec základného predplatného, ktoré tu nie je uvedené a buď je momentálne dostupné alebo vo fáze vývoja, sa nepovažuje za aktualizáciu a musí byť pridelené samostatne.

1.6 Definície

Majiteľ konta – je koncový užívateľ Zákazníka, ktorý nainštaloval klientsky aktivačný softvér, akceptoval licenčnú zmluvu koncového užívateľa a aspoň raz sa autentifikoval v Maloobchodnej alebo Podnikovej aplikácii Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS.

Klientsky softvér Majiteľa konta – je klientsky aktivačný softvér IBM Security Trusteer Rapport alebo klientsky aktivačný softvér IBM Security Trusteer Mobile Browser alebo iný klientsky aktivačný softvér, ktorý sa dodáva s niektorými predplatnými služieb IBM SaaS na inštaláciu do zariadenia koncového užívateľa.

Úvodná stránka Trusteer – je úvodná stránka, ktorá sa Zákazníkovi poskytuje na základe dostupných šablón úvodných stránok.

Cieľová stránka – je stránka, ktorej hostiteľom je IBM a ktorá sa zákazníkovi poskytuje s úvodnou stránkou Zákazníka a so stiahnuteľným Klientskym softvérom Majiteľa konta.

2. Ponuky IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail a/alebo IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport ochrannú vrstvu voči phishingu a malvérovým útokom MitB (Man-in-the-Browser). S využitím siete desiatok miliónov koncových bodov po celom svete zhromažďuje IBM Security Trusteer Rapport podrobné informácie o aktívnych phishingových a malvérových útokoch voči organizáciám po celom svete. IBM Security Trusteer Rapport používa behaviorálny algoritmus určený na blokovanie phishingových útokov a na zamedzenie inštalácie a prevádzky variant malvéru MitB.

Táto ponuka IBM SaaS má metriku spoplatňovania Oprávnených účastníkov. Ponuka s označením Business sa predáva v balíkoch po 10 Oprávnených účastníkoch. Ponuka s označením Retail sa predáva v balíkoch po 100 Oprávnených účastníkoch.

Táto ponuka služby IBM SaaS zahŕňa:

a. Trusteer Management Application ("TMA"):

Služba TMA sa poskytuje v rámci cloudového prostredia produktu IBM Security Trusteer, prostredníctvom ktorého môže Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov): (i) prijímať hlásenia s údajmi udalostí a posúdenia rizík, (ii) prezerať, konfigurovať a nastaviť bezpečnostné politiky a politiky súvisiace s nahlasovaním údajov udalostí a (iii) zobraziť konfiguráciu klientskeho aktivačného softvéru, licencia pre ktorý sa na základe licenčnej zmluvy koncového užívateľa poskytuje verejnosti bezplatne a ktorý sa sprístupní na stiahnutie do osobných počítačov alebo zariadení (PC/MAC) Oprávnených účastníkov, nazývané tiež balík softvéru Trusteer Rapport (ďalej len „Klientsky softvér Majiteľa konta“). Zákazník môže Klientsky softvér Majiteľa účtu poskytovať len s Úvodnou stránkou Trusteer alebo rozhraním Rapport API a Zákazník nesmie Klientsky softvér Majiteľa účtu používať na svoju internú podnikovú prevádzku ani ho nesmú používať zamestnanci (na iné ako osobné použitie zamestnancov).

b. Webové skripty:

Pre prístup na webové stránky za účelom pristupovania na alebo používania ponúk IBM SaaS.

c. Údaje udalostí:

Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie údajov udalostí vygenerovaných z Klientskeho softvéru Majiteľa konta v dôsledku online transakcií Majiteľa konta s jeho Podnikovou alebo Maloobchodnou aplikáciou, pre ktorú si Zákazník predplatil službu IBM SaaS. Údaje udalostí sa budú prijímať z Klientskeho softvéru Majiteľa konta, ktorý sa spúšťa na zariadeniach Oprávnených účastníkov, ktorí akceptovali licenčnú zmluvu koncového užívateľa a aspoň raz sa autentifikovali v Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pričom konfigurácia Zákazníka musí obsahovať kolekciu ID užívateľov.

d. Trusteer Splash:

Marketingová platforma Trusteer Splash identifikuje a poskytuje Klientsky softvér Majiteľa konta Oprávneným účastníkom, ktorí pristupujú k Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS. Zákazník si môže vybrať z dostupných Šablón Úvodných stránok. Zákazník môže zakúpiť prispôsobenie úvodnej stránky na základe osobitnej zmluvy alebo zmluvy o dielo.

Zákazník môže súhlasiť s poskytnutím svojich ochranných známok, log alebo ikon na použitie v spojitosti so službou TMA a to výhradne na použitie s platformou Trusteer Splash a na zobrazenie v Klientskom softvéri Majiteľa konta alebo na cieľových stránkach, ktorých hostiteľom je IBM, a na webovej stránke IBM Security Trusteer. Každé použitie ním poskytnutých ochranných známok, log alebo ikon bude v súlade s náležitými politikami IBM ohľadom reklamy a použitia ochranných známok.

V prípade, že Zákazník chce použiť ľubovoľný typ povinného nasadenia Klientskeho softvéru Majiteľa konta, musí si predplatiť službu IBM Security Trusteer Rapport Mandatory Service SaaS.

Povinné nasadenie Klientskeho softvéru Majiteľa konta zahŕňa, ale nie je obmedzené na, ľubovoľný typ povinného nasadenia pomocou ľubovoľného mechanizmu alebo prostriedkov, ktoré priamo alebo nepriamo nútia Oprávneného účastníka stiahnuť si Klientsky softvér Majiteľa konta, alebo akúkoľvek metódu, nástroj, postup, zmluvu alebo mechanizmus, ktoré neboli vytvorené alebo schválené IBM a ktorých účelom je obísť licenčné požiadavky tohto povinného nasadenia Klientskeho softvéru Majiteľa konta.

2.2 Voliteľné Dodatočné ponuky IBM SaaS pre IBM Security Trusteer Rapport for Business a/alebo pre IBM Security Trusteer Rapport for Retail

Predplatné pre ponuky IBM Security Trusteer Rapport je nevyhnutnou podmienkou pre predplatné k nasledujúcim dodatočným ponukám IBM SaaS. Ak je IBM SaaS označený ako "for Business", potom musí byť kúpená dodatočná ponuka IBM SaaS tiež označená ako "for Business". Ak je IBM SaaS označený ako "for Retail", potom musí byť kúpená dodatočná ponuka IBM SaaS tiež označená ako "for Retail". Zákazníkovi sa budú posielať údaje udalostí od Oprávnených účastníkov, ktorí spúšťajú Klientsky softvér Majiteľa konta, akceptovali licenčnú zmluvu koncového užívateľa a aspoň raz sa autentifikovali v Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pričom konfigurácia Zákazníka musí obsahovať kolekciu ID užívateľov.

2.2.1 IBM Security Trusteer Fraud Feeds for Business a/alebo IBM Security Trusteer Rapport Fraud Feeds for Retail

Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie údajov udalostí súvisiacich s infekciami malvérom a s inými bezpečnostnými udalosťami v koncových bodoch na konkrétnej pracovnej stanici Majiteľa.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business a/alebo IBM Security Trusteer Rapport Phishing Protection for Retail

Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie oznámení o údajoch udalostí súvisiacich s odovzdaním prihlasovacích údajov Majiteľa konta na podozrivej phishingovej alebo potenciálne podvodnej lokalite. Legitímne online aplikácie (adresy URL) môžu byť omylom označené ako phishingové lokality a IBM SaaS môže vystríhať Majiteľov kont, že legitímna lokalita je phishingová lokalita. V takomto prípade musí Zákazník spoločnosti IBM tento omyl oznámiť a IBM musí chybu opraviť. Toto bude jediný nápravný mechanizmus Zákazníka v prípade takejto chyby.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business a/alebo IBM Security Trusteer Rapport Mandatory Service for Retail

Zákazník môže inštanciu marketingovej platformy Trusteer Splash použiť na nariadenie stiahnutia Klientskeho softvéru Majiteľa konta Oprávneným účastníkom, ktorí pristupujú k Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS.

IBM Security Trusteer Rapport Premium Support for Business je nevyhnutnou podmienkou k IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail je nevyhnutnou podmienkou k IBM Security Rapport Mandatory Service for Retail.

Zákazník môže implementovať ďalšie funkcie produktu IBM Security Trusteer Rapport Mandatory Service len vtedy, ak boli objednané a nakonfigurované na používanie so Zákazníkovou Maloobchodnou alebo Podnikovou aplikáciou, pre ktorú si Zákazník predplatil službu IBM SaaS.

3. Ponuky IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint je cloudová služba, ktorá je navrhnutá tak, aby poskytovala ďalšiu vrstvu ochrany a je zameraná, aby zisťovala a zmierňovala útoky malvéru, phishingové útoky a útoky prebratia konta. Služba Trusteer Pinpoint sa môže integrovať do Podnikových alebo Maloobchodných aplikácií Zákazníka, pre ktoré si Zákazník predplatil služby IBM SaaS a procesy prevencie podvodných aktivít.

Táto ponuka služby IBM SaaS zahŕňa:

a. TMA:

   Služba TMA je k dispozícii v cloudovom prostredí produktu IBM Security Trusteer, prostredníctvom ktorého môže Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov): (i) prijímať hlásenia s údajmi udalostí a posúdenia rizík, (ii) prezerať, konfigurovať a nastaviť bezpečnostné politiky a politiky súvisiace s nahlasovaním údajov udalostí.

b. Webový skript a/alebo rozhrania API:

   Pre nasadenie na webové stránky za účelom pristupovania na alebo používania IBM SaaS.

3.1 IBM Security Trusteer Pinpoint Malware Detection a IBM Security Trusteer Pinpoint Criminal Detection

V prípade, že služby IBM Security Trusteer Pinpoint Malware Detection zistia malvér alebo služby IBM Security Trusteer Pinpoint Criminal Detection zistia, že bolo ovládnuté konto, Zákazník musí postupovať podľa pokynov v príručke Pinpoint Best Practices Guide. Zákazník nesmie nikdy používať službu IBM Security Trusteer Pinpoint Malware Detection alebo IBM Security Trusteer Pinpoint Criminal Detection spôsobom, ktorý by ovplyvnil skúsenosti Oprávneného účastníka hneď po zistení malvéru alebo ovládnutia konta, čiže spôsobom, na základe ktorého by bolo možné spojiť akcie Zákazníka s používaním služieb IBM Security Trusteer Pinpoint (napríklad oznámenia, správy, blokovanie zariadení alebo blokovanie prístupu k Podnikovej alebo Maloobchodnej aplikácii ihneď po zistení malvéru alebo ovládnutia konta).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business a/alebo IBM Security Trusteer Pinpoint Criminal Detection for Retail

Bezklientske zisťovanie podozrivej činnosti ovládnutia konta v prehliadačoch, ktoré sa pripájajú k Podnikovej alebo Maloobchodnej Aplikácii, s použitím ID zariadenia, zisťovania phishingu a zisťovania krádeže prihlasovacích údajov iniciovanej malvérom. Ponuky IBM Security Trusteer Pinpoint Criminal Detection poskytujú Zákazníkovi ďalšiu vrstvu ochrany a sú určené na zisťovanie pokusov o ovládnutie kont a poskytovanie hodnotenia rizikovosti prehliadačov alebo mobilných zariadení (prostredníctvom natívneho prehliadača alebo zákazníckej mobilnej aplikácie), ktoré sa priamo pripájajú k Podnikovej alebo Maloobchodnej aplikácii.

a. Údaje udalostí:

   Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie údajov udalostí, ktoré boli vygenerované v dôsledku online interakcií Oprávneného účastníka so Zákazníkovou Podnikovou alebo Maloobchodnou aplikáciou (alebo aplikáciami), pre ktorú si Zákazník predplatil službu IBM SaaS, alebo Zákazník môže prijímať údaje udalostí v režime doručovania cez koncové rozhranie API.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile alebo IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Služby IBM Security Trusteer Pinpoint Criminal Detection for Mobile (PPCD Mobile) sú navrhnuté tak, aby poskytovali Zákazníkovi ďalšiu úroveň ochrany a chránili ho pred ovládnutím konta a podvodnými aktivitami identifikáciou neoprávneného prístupu ku kontám a poskytovaním odporúčaní Zákazníkovi. Táto služba IBM SaaS zhromažďuje informácie pochádzajúce z Podnikovej alebo Maloobchodnej aplikácie Zákazníka prostredníctvom rozhrania PPCD Mobile API, ako aj z mobilných zariadení Oprávnených účastníkov. Služby IBM Security Trusteer PPCD Mobile sú navrhnuté tak, aby dali do súvisu komplexné informácie súvisiace s mobilnými zariadeniami Oprávnených účastníkov s inými zdrojmi údajov, ako sú informácie o udalostiach infekcie malvérom a phishingu integrované cez iné ponuky IBM SaaS IBM Security Trusteer uvedené v týchto Podmienkach používania.

Zákazník môže pristupovať k službám IBM Security Trusteer PPCD Mobile v cloudovom prostredí produktu IBM Security Trusteer a prijímať údaje hodnotení rizík z mobilných zariadení Oprávnených účastníkov vygenerované v dôsledku online interakcií týchto mobilných zariadení s Podnikovou alebo Maloobchodnou aplikáciou Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS. Na účely týchto služieb budú „mobilné zariadenia“ zahŕňať iba podporované mobilné telefóny a tablety, nie však počítače PC alebo MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Bezklientske zisťovanie prehliadačov infikovaných finančným malvérom MitB (Man in the Browser), ktoré sa pripájajú k Podnikovej a/alebo Maloobchodnej Aplikácii. Služby IBM Security Trusteer Pinpoint Malware Detection poskytujú ďalšiu vrstvu ochrany a umožňujú organizáciám zamerať sa na procesy zamedzovania podvodom na základe rizikovosti malvéru, pričom Zákazníkom poskytujú hodnotenia a výstrahy týkajúce sa prítomnosti finančného malvéru MitB.

a. Údaje udalostí:

   Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie údajov udalostí, ktoré boli vygenerované v dôsledku online interakcií Oprávnených účastníkov s Podnikovou alebo Maloobchodnou aplikáciou (aplikáciami) Zákazníka.

b. Rozšírené vydanie:

   Vydania Advanced Edition for Business alebo Advanced Edition for Retail ponúkajú ďalšiu vrstvu zisťovania a ochrany, ktorá sa prispôsobí štruktúre a toku údajov Zákazníkových Podnikových alebo Maloobchodných aplikácií a je ich možné prispôsobiť špecifickej skupine ohrození namierených proti Zákazníkovi. Je ich možné začleniť na rôzne miesta v Zákazníkových Podnikových alebo Maloobchodných aplikáciách.

   Vydania Advanced Edition sa Zákazníkovi ponúkajú v minimálnom množstve 100 000 Oprávnených účastníkov pre vydanie Retail alebo 10 000 Oprávnených účastníkov pre vydanie Business, čo

predstavuje 1000 balíkov po 100 Oprávnených účastníkoch pre vydanie Retail alebo 1000 balíkov po 10 Oprávnených účastníkoch pre vydanie Business.

c. Štandardné vydanie:

Štandardné vydanie pre Podnik alebo pre Maloobchod je rýchlo nasaditeľné riešenie, ktoré poskytuje hlavnú funkčnosť tejto popisovanej ponuky IBM SaaS.

3.2 Voliteľné Dodatkové ponuky IBM SaaS pre IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition a/alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pri ponukách IBM Security Trusteer Rapport Remediation for Retail existuje nevyhnutná podmienka mať IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

Pri IBM Security Trusteer Pinpoint Carbon Copy for Retail existuje nevyhnutná podmienka mať IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition alebo IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Pri IBM Security Trusteer Pinpoint Carbon Copy for Business existuje nevyhnutná podmienka mať IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition alebo IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business a/alebo IBM Security Trusteer Pinpoint Carbon Copy for Retail

Služby IBM Security Trusteer Pinpoint Carbon Copy sú navrhnuté tak, aby poskytovali ďalšiu vrstvu ochrany a službu monitorovania, ktorá pomáha zistiť čas, kedy boli prihlasovacie údaje Oprávneného účastníka vyzradené prostredníctvom phishingových útokov na Zákazníkove Maloobchodné alebo Podnikové aplikácie, pre ktoré si Zákazník predplatil službu IBM SaaS.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

Cieľom služby IBM Security Trusteer Rapport Remediation for Retail je vyšetrovať, vyriešiť, blokovať a odstraňovať infekcie malvérom MitB (man-in-the-browser) z infikovaných zariadení (PC/MAC) Oprávnených účastníkov Zákazníka, ktorí pristupujú k Maloobchodnej aplikácii Zákazníkovu sporadicky, pričom infekcie malvérom MitB boli zistené na základe údajov udalostí služby IBM Security Trusteer Pinpoint Malware Detection. Zákazník musí mať platné predplatné služby IBM Security Trusteer Pinpoint Malware Detection, pričom táto služba musí byť skutočne spustená v Maloobchodnej aplikácii Zákazníka. Zákazník môže túto služby IBM SaaS používať len v spojitosti s Oprávnenými účastníkmi, ktorí pristupujú k Maloobchodnej aplikácii Zákazníka, a výhradne ako nástroj určený na vyšetrovanie a nápravu konkrétnych infikovaných zariadení (PC/MAC). Služba IBM Security Trusteer Rapport Remediation for Retail musí byť spustená v príslušnom ovplyvnenom zariadení (PC/MAC) Oprávneného účastníka, pričom takto ovplyvnený Oprávnený účastník musí akceptovať licenčnú zmluvu koncového užívateľa, autentifikovať sa aspoň raz v Maloobchodnej aplikácii (aplikáciách) Zákazníka, a konfigurácia Zákazníka musí zahŕňať kolekciu ID užívateľov. Aby sa vylúčili všetky pochybnosti, táto ponuka služby IBM SaaS nezahŕňa oprávnenie používať službu Trusteer Splash alebo všeobecne sprístupniť Klientsky softvér Majiteľa konta Oprávneným účastníkom Zákazníka akýmkoľvek iným spôsobom.

4. Ponuky IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business a/alebo IBM Security Trusteer Mobile Browser for Retail

Služba IBM Security Trusteer Mobile Browser je navrhnutá tak, aby poskytovala ďalšiu vrstvu ochrany, pričom zabezpečuje bezpečný online prístup k mobilným zariadeniam Oprávnených účastníkov, ktorí pristupujú k Maloobchodným alebo Podnikovým aplikáciám Zákazníka, pre ktoré si Zákazník predplatil službu IBM SaaS, poskytuje hodnotenie rizikovosti mobilných zariadení a zaručuje ochranu pred phishingom. Bezpečné zisťovanie cez Wi-Fi je k dispozícii len pre platformy Android. Na účely tejto ponuky IBM SaaS boli zahrnuté mobilné zariadenia, mobilné telefóny alebo tablety a neboli zahrnuté Prenosné počítače, PC a počítače MAC.

Prostredníctvom služby TMA môže Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) prijímať údaje udalostí, analýzy a štatistické informácie týkajúce sa Zariadení, ktorých Oprávnení účastníci: (i) si bezplatne stiahli Klientsky softvér Majiteľa konta, aplikáciu s verejnou licenciou na základe

licenčnej zmluvy koncového užívateľa a poskytli ho na stiahnutie na mobilné zariadenia Oprávnených účastníkov a (ii) akceptovali licenčnú zmluvu koncového užívateľa a aspoň raz sa autentifikovali v Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS. Zákazník môže Klientsky softvér Majiteľa účtu poskytovať len s Úvodnou stránkou Trusteer a Zákazník nesmie Klientsky softvér Majiteľa účtu používať pri svojich interných obchodných operáciách.

a. Údaje udalostí:

   Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) môže používať produkt TMA na prijímanie údajov udalostí vygenerovaných v dôsledku online interakcií mobilných zariadení s Maloobchodnými alebo Podnikovými aplikáciami Zákazníka, pre ktoré si Zákazník predplatil službu IBM SaaS.

b. Trusteer Splash:

   Marketingová platforma Trusteer Splash identifikuje a poskytuje Klientsky softvér Majiteľa konta Oprávneným účastníkom, ktorí pristupujú k Podnikovej alebo Maloobchodnej aplikácii Zákazníka, pre ktorú si Zákazník predplatil službu IBM SaaS. Zákazník si môže vybrať z dostupných šablón úvodných stránok (ďalej len „Šablóna úvodnej stránky“). Zákazník môže zakúpiť prispôsobenie úvodnej stránky na základe osobitnej zmluvy alebo zmluvy o dielo.

Zákazník môže súhlasiť s poskytnutím svojich ochranných známok, log alebo ikon na použitie v spojitosti so službou TMA a to výhradne na použitie s platformou Trusteer Splash a na zobrazenie v Klientskom softvéri Majiteľa konta alebo na cieľových stránkach, ktorých hostiteľom je IBM, alebo na webovej stránke IBM Security Trusteer. Každé použitie ním poskytnutých ochranných známok, log alebo ikon bude v súlade s náležitými politikami IBM ohľadom reklamy a použitia ochranných známok.

4.2 IBM Security Trusteer Mobile SDK for Business a/alebo IBM Security Trusteer Mobile SDK for Retail

Ponuky služieb IBM Security Trusteer Mobile SDK sú navrhnuté tak, aby poskytovali ďalšiu vrstvu ochrany a zabezpečili bezpečný webový prístup k Podnikovým alebo Maloobchodným aplikáciám Zákazníka, pre ktoré si Zákazník predplatil službu IBM SaaS, hodnotenie rizikovosti zariadení a ochranu pred pharmingom. Bezpečné zisťovanie cez Wi-Fi je k dispozícii len pre platformy Android.

Ponuky služieb IBM Security Trusteer Mobile SDK obsahujú vlastnú množinu nástrojov na vývoj mobilného softvéru (ďalej len „SDK“), softvérový balík obsahujúci dokumentáciu, vlastné programovacie softvérové knižnice a iné súvisiace súbory a položky, známe ako mobilná knižnica IBM Security Trusteer, ako aj „Komponent prostredia runtime“ alebo „Redistributovateľný balík“, vlastný kód generovaný službou IBM Security Trusteer Mobile SDK, ktorý je možné vložiť a integrovať do Zákazníkových chránených samostatných mobilných aplikácií iOS alebo Android, pre ktoré si Zákazník predplatil službu IBM SaaS (ďalej len „Zákazníkom integrované mobilné aplikácie“).

IBM Security Trusteer Mobile SDK for Retail je k dispozícii v balíkoch po 100 Oprávnených účastníkoch alebo v balíkoch po 100 Klientskych zariadeniach a IBM Security Trusteer Mobile SDK for Business je k dispozícii v balíkoch po 10 Oprávnených účastníkoch alebo v balíkoch po 10 Klientskych zariadeniach.

Prostredníctvom služby TMA môže Zákazník (a neobmedzený počet jeho autorizovaných pracovníkov) prijímať zostavy s údajmi udalostí a hodnotenia trendov rizík. Prostredníctvom Zákazníkom integrovanej mobilnej aplikácie môže Zákazník prijímať informácie z analýzy rizík a informácie o mobilných zariadeniach súvisiace s mobilnými zariadeniami Spôsobilých účastníkov, ktorí si stiahli Zákazníkom integrovanú mobilnú aplikáciu, vďaka čomu môže Zákazník vybudovať svoju vlastnú politiku ochrany pred podvodmi uplatňujúcu opatrenia na minimalizáciu týchto rizík. Na účely tejto služby budú „mobilné zariadenia“ zahŕňať iba podporované mobilné telefóny a tablety, nie však počítače PC alebo MAC.

Zákazník môže:

a. interne používať službu IBM Security Trusteer Mobile SDK výhradne na účely vývoja Zákazníkom integrovanej mobilnej aplikácie;

b. zahrnúť Redistribuovateľný balík (výhradne vo formáte objektového kódu) ako neoddeliteľnú súčasť do Zákazníkom integrovanej mobilnej aplikácie. Každá upravená alebo zlúčená časť Redistributovateľnej aplikácie bude na základe udelenia tejto licencie podliehať podmienkam tejto ToU; a

c. predávať a distribuovať Redistribuovateľnú aplikáciu prostredníctvom sťahovania do mobilných zariadení Oprávnených účastníkov alebo do Klientskeho zariadenia vlastníka pod podmienkou, že:

- Pokiaľ to táto Zmluva výslovne nepovoľuje, Zákazník (1) nesmie používať, kopírovať, upravovať alebo distribuovať balík SDK; (2) nesmie spätne zostavovať, spätne kompilovať alebo iným spôsobom prekladať balík SDK alebo vykonávať úkony spätného inžinierstva, pokiaľ to výslovne nepovoľujú platné právne predpisy bez možnosti zmluvného zrieknutia sa tohto práva; (3) nesmie udeľovať podriadené licencie na balík SDK, dať ho do prenájmu alebo nájmu; (4) nesmie odstrániť žiadne informácie o autorských právach alebo súbory s právnymi vyhláseniami z Redistribuovateľného balíka; (5) nesmie používať rovnakú cestu ako mali súbory/moduly v pôvodnom Redistribuovateľnom balíku a (6) nesmie používať názvy alebo ochranné známky IBM, jej poskytovateľov licencií alebo distribútorov v súvislosti s predajom Zákazníkom integrovanej mobilnej aplikácie bez predchádzajúceho písomného súhlasu IBM alebo príslušného poskytovateľa licencie alebo distribútora.
- Redistribuovateľný balík musí zostať neoddeliteľnou súčasťou Zákazníkom integrovanej mobilnej aplikácie. Redistribuovateľný balík môže byť výhradne vo forme objektového kódu a musí byť v súlade so všetkými usmerneniami, pokynmi a špecifikáciami definovanými v balíku SDK a dokumentácii k tomuto balíku. Licenčná zmluva koncového užívateľa vzťahujúca sa na Klientom integrovanú mobilnú aplikáciu musí upozorňovať koncových užívateľov na to, že Redistribuovateľný balík sa nesmie i) používať na žiadne iné účely ako na podporu Klientom integrovanej mobilnej aplikácie ii) kopírovať (okrem vytvárania záložných kópií), iii) ďalej distribuovať alebo prenášať iv) spätne zostavovať, spätne kompilovať alebo iným spôsobom prekladať, pokiaľ to výslovne nepovoľujú platné právne predpisy bez možnosti zmluvného zrieknutia sa tohto práva. Licenčná zmluva Zákazníka musí chrániť IBM prinajmenšom v rovnakej miere ako podmienky tejto Zmluvy.
- Balík SDK sa môže nasadiť výhradne na účely interného vývoja a testovania Zákazníka na testovacích mobilných zariadeniach určených Zákazníkom. Zákazník nesmie balík SDK využívať pri spracovaní produkčných pracovných zaťažení, simulácii produkčných pracovných zaťažení alebo testovaní rozšíriteľnosti akéhokoľvek kódu, aplikácie alebo systému. Zákazník nesmie žiadnu časť balíka SDK používať na žiadne iné účely.

Zákazník bude niesť zodpovednosť za všetku technickú podporu súvisiacu so Zákazníkom integrovanou mobilnou aplikáciou a všetky úpravy v Redistribuovateľných balíkoch vykonaných Zákazníkom povolené na základe tejto Zmluvy.

Zákazník môže nainštalovať a používať Redistribuovateľné balíky a balík IBM Security Mobile SDK iba na účely podpory používania služby IBM SaaS Zákazníkom.

IBM otestovala vzorové aplikácie vytvorené pomocou mobilných nástrojov, obsiahnutých v IBM Security Trusteer Mobile SDK ("Mobilné nástroje"), aby zistila, či sa budú správne spúšťať na určitých verziách platforiem mobilných operačných systémov od Apple (iOS), Google (Android) a iných výrobcov (spoločne nazývaných "Platformy mobilných OS"), Platformy mobilných OS dodávajú však tretie strany, ktoré nie sú riadené IBM a môžu sa meniť bez toho, aby o tom bola spoločnosť IBM informovaná. Bez ohľadu na akékoľvek protichodné ustanovenia, spoločnosť IBM nezaručuje, že aplikácie alebo iný výstup vytvorený pomocou Mobilných nástrojov sa budú správne vykonávať na všetkých Platformách mobilných operačných systémov alebo mobilných zariadeniach, budú s nimi spolupracovať alebo budú s nimi kompatibilné.

Zákazník súhlasí, že bude vytvárať, uchovávať a poskytovať spoločnosti IBM a jej audítorom presné písomné záznamy, výstupy zo systémových nástrojov a iné systémové informácie, ktoré budú postačujúce na to, aby IBM v rámci auditu dokázala overiť, či Zákazník používa balík IBM Security Trusteer Mobile SDK v súlade s ustanoveniami týchto Podmienok používania.

5. Nasadenie ponúk IBM SaaS Fraud Protection

Základné predplatné Zákazníka zahŕňa vyžadované nastavenie a činnosti pri prvom nasadení vrátane úvodného jednorazového nastavenia, konfigurácie, Šablóny úvodnej stránky, testovania a školenia.

Ďalšie služby sa dajú zazmluvniť za príplatok prostredníctvom osobitnej zmluvy.

Príloha B

IBM poskytuje nasledujúcu Zmluvu o úrovni poskytovaných služieb („SLA“) vo vzťahu k dostupnosti služby IBM SaaS, pričom táto zmluva sa uplatňuje v prípade, ak je tak uvedené v Transakčnom dokumente Zákazníka:

Bude sa uplatňovať tá verzia Zmluvy o úrovni poskytovaných služieb, ktorá bude v platnosti na začiatku Doby predplatného Zákazníka alebo v čase jej obnovenia. Zákazník berie na vedomie, že Zmluva o úrovni poskytovaných služieb nepredstavuje záruku.

1. Definície

a. **Oprávnená kontaktná osoba** – je jednotlivec, ktorého Zákazník uviedol spoločnosti IBM ako osobu, ktorá má oprávnenie odovzdávať Žiadosti na základe tejto Zmluvy o úrovni poskytovaných služieb.

b. **Kredit za nedostupnosť** – znamená náprava, akú IBM poskytne za platnú Reklamáciu. Kredit za nedostupnosť sa uplatní vo forme dobropisu alebo zľavy z budúcej faktúry za poplatky za predplatné služby IBM SaaS.

c. **Žiadosť** – predstavuje sťažnosť doručenú IBM zo strany Oprávnenej kontaktnej osoby Zákazníka v súlade so Zmluvou o úrovni poskytovaných služieb a v súvislosti s nesplnením Úrovne služieb za Zmluvný mesiac.

d. **Zmluvný mesiac** – predstavuje jednotlivý úplný mesiac počas obdobia poskytovania služby IBM SaaS, začínajúci 00:00 CET (stredoeurópskeho času) v prvý deň mesiaca a končiaci 23:59 CET (stredoeurópskeho času) v posledný deň mesiaca.

e. **Zákazník** – znamená subjekt, ktorý si službu IBM SaaS predplatil priamo u IBM a ktorý nie je v omeškaní s plnením svojich vecných záväzkov, vrátane platobných povinností na základe tejto zmluvy s IBM pre službu IBM SaaS.

f. **Doba výpadku** – predstavuje časový úsek, počas ktorého prestal fungovať produkčný systém určený na spracovanie Služby a žiaden z užívateľov nie je schopný využívať žiaden z aspektov Služby, na ktoré majú príslušné oprávnenia. Doba výpadku nezahŕňa časové obdobie, počas ktorého Služba nebola dostupná v dôsledku:

- plánovanej nedostupnosti systémov
- vyššej moci
- problémov s aplikáciami, zariadením alebo údajmi Klienta alebo tretích strán
- pochybení alebo zanedbaní zo strany zákazníka alebo tretej strany (vrátane získania prístupu k Službe inými osobami prostredníctvom hesla alebo zariadenia)
- nesplnenia požiadaviek konfigurácie systémov a podporovaných platforiem, ktoré sú vyžadované pri prístupe k Službe IBM SaaS
- toho, že IBM dodrží súlad s návrhmi, špecifikáciami alebo pokynmi, ktoré jej poskytne Klient alebo tretia strana v mene Klienta.

g. **Udalosť** – predstavuje okolnosť alebo súbor súvisiacich okolností, v dôsledku ktorých nebolo možné dosiahnuť Úroveň poskytovanej služby.

h. **Vyššia moc** – znamená Boží zásah (nezavinenú udalosť), terorizmus, odborársky protest, požiar, záplavy, zemetrasenie, povstanie, vojnu, vládne zásahy alebo príkazy alebo obmedzenia, vírusy, útoky zamerané na zneprístupnenie služby (tzv. Denial of Service) a iné škodlivé správanie, zlyhania pripojenia k verejným a počítačovým sieťam a iné príčiny nedostupnosti služby IBM SaaS, ktorým IBM nemohla zamedziť.

i. **Plánovaná nedostupnosť systémov** – znamená plánované prerušenie poskytovania služby IBM SaaS za účelom servisnej údržby.

j. **Úroveň poskytovanej služby** – predstavuje nižšie definovaný štandard, na základe ktorého spoločnosť IBM meria úroveň služby, ktorú poskytuje podľa tejto SLA.

2. Kredity za nedostupnosť

a. Aby Zákazník získal oprávnenie na podanie žiadosti, musí mať zaznamenaný lístok podpory pre všetky Udalosti na oddelení technickej podpory spoločnosti IBM pre príslušnú službu IBM SaaS, v súlade s predpismi spoločnosti IBM týkajúcimi sa ohlasovania problémov so závažnosťou 1. Zákazník musí poskytnúť všetky vyžadované podrobné informácie o Udalosti a v primeranej miere pomôcť spoločnosti IBM pri diagnostike a riešení Udalosti v rozsahu vyžadovanom pre lístky podpory problémov so závažnosťou 1. Tieto lístky musia byť zaznamenané v priebehu dvadsiatich štyroch hodín (24) od prvého zistenia, že Udalosť mala dopad na používanie služby Zákazníkom.

b. Oprávnená kontaktná osoba Zákazníka je povinná predložiť Žiadosť o Kredit za nedostupnosť najneskôr do 3 pracovných dní od uplynutia Zmluvného mesiaca, ktorý je predmetom Žiadosti.

c. Oprávnená kontaktná osoba Zákazníka musí spoločnosti IBM poskytnúť všetky príslušné podrobnosti týkajúce sa žiadosti vrátane, ale bez obmedzenia na, podrobných popisov všetkých relevantných Udalostí a Úrovne služieb, ktorá údajne nebola splnená.

d. Spoločnosť za každý Zmluvný mesiac interne odmeria celkovú kombinovanú Dobu výpadku, ktorá sa vzťahuje na príslušnú Úroveň služieb uvedenú v tabuľke nižšie. Kredity za nedostupnosť sa budú udeľovať na základe trvania Doby výpadku meraného od času, ktorý Zákazník nahlási ako čas prvého výskytu Doby výpadku. Ak Klient nahlási Udalosť výpadku aplikácie simultánnu s Udalosťou výpadku spracovania vstupných údajov, spoločnosť IBM bude prekrývajúce sa obdobia Doby výpadku považovať za jedno obdobie Doby výpadku, a nie za dve samostatné obdobia Doby výpadku. Za každú platnú Žiadosť spoločnosť IBM udelí najvyšší možný Kredit za nedostupnosť na základe dosiahnutej Úrovne služieb za daný Zmluvný mesiac, ako je uvedené v tabuľkách nižšie. Spoločnosť IBM neudelí viacero Kreditov za nedostupnosť v súvislosti s rovnakou Udalosťou v priebehu jedného Zmluvného mesiaca.

e. Pri Združenej službe (jednotlivé IBM SaaS zabalené a predávané spoločne za jednu kombinovanú cenu) bude Kredit za nedostupnosť vypočítaný na základe jednej kombinovanej mesačnej ceny za Združenú službu a nie na základe poplatku mesačného predplatného pre každú jednotlivú IBM SaaS. Zákazník môže odosielať len Žiadosti súvisiace s jednou samostatnou službou IBM SaaS v rámci balíka služieb v ľubovoľnom Zmluvnom mesiaci a IBM nebude povinná udeliť Kredity za nedostupnosť v súvislosti s viacerými službami IBM SaaS v balíku služieb za ľubovoľný Zmluvný mesiac.

f. Ak Zákazník zakúpil službu IBM SaaS od oprávneného predajcu IBM v rámci remarketingovej transakcie, pri ktorej si IBM zachová primárnu zodpovednosť za plnenie záväzkov súvisiacich so službou IBM SaaS a v oblasti úrovne poskytovaných služieb, potom sa bude Kredit za nedostupnosť odvíjať od ceny RSVP (Relationship Suggested Value Price) platnej v danom čase pre službu IBM SaaS za Zmluvný mesiac, ktorý je predmetom Žiadosti, so zľavou 50 %.

g. Celkový počet Kreditov za nedostupnosť udelených v ľubovoľnom Zmluvnom mesiaci za žiadnych okolností nesmie prekročiť desať percent (10 %) jednej dvanástiny (1/12) ročného poplatku, ktorý Zákazník uhradí IBM za službu IBM SaaS.

h. Spoločnosť IBM primerane zváži Žiadosti na základe údajov dostupných v záznamoch spoločnosti IBM, ktoré sa uprednostnia v prípade nesúladu s údajmi v záznamoch Zákazníka.

i. KREDITY ZA NEDOSTUPNOSŤ, KTORÉ SA ZÁKAZNÍKOVI UDELIA NA ZÁKLADE TEJTO ZMLUVY O ÚROVNI POSKYTOVANÝCH SLUŽIEB, PREDSTAVUJÚ JEDINÝ A VÝLUČNÝ NÁPRAVNÝ PROSTRIEDOK V SÚVISLOSTI S AKÝMIKOĽVEK ŽIADOSŤAMI.

3. Úrovne služieb

Dostupnosť služby IBM SaaS počas Zmluvného mesiaca

Dosiahnutá úroveň služieb (počas Zmluvného mesiaca)	**Kredit za nedostupnosť (% mesačného Predplatného za Zmluvný mesiac, ktorého sa Žiadosť týka)**
< 99,5%	2 %
< 98,0%	5 %
< 96,0%	10 %

"Dosiahnutá úroveň služieb" vyjadrená v percentách, sa vypočíta ako : (a) celkový počet minút v Zmluvnom mesiaci mínus (b) celkový počet minút Doby výpadku v Zmluvnom mesiaci, deleno (c) celkovým počtom minút v Zmluvnom mesiaci.

Napríklad: celkovo 250 minút Doby výpadku počas Zmluvného mesiaca

Celkovo 43 200 minút v Zmluvnom mesiaci (30 dní) - 250 minút Doby výpadku = 42 950 minút _____ 43 200 celkových minút	= 2 % Kredit za nedostupnosť pre dosiahnutú Úroveň služieb na úrovni 99,4 % počas Zmluvného mesiaca

3.1 Vylúčenia

Táto Zmluva o úrovni poskytovaných služieb sa poskytuje iba Zákazníkom IMB. Táto Zmluva o úrovni poskytovaných služieb sa nevzťahuje na:

- služby vo verzii Beta a skúšobné verzie služieb
- neprodukčné prostredia vrátane, ale bez obmedzenia na, testovacích prostredí, prostredí na zotavenie po havárii, prostredí na kontrolu kvality alebo vývojových prostredí
- Žiadosti podané užívateľmi, hosťami, účastníkmi a oprávnenými pozvanými účastníkmi v službe IBM SaaS Zákazníka
- v prípade závažného porušenia povinností vyplývajúcich z týchto Podmienok používania zo strany Zákazníka vrátane, ale bez obmedzenia na, porušenia platobných povinností