IBM Security Trusteer Fraud Protection

Vilkår for brug består af disse IBM Vilkår for brug – SaaS-specifikke produktvilkår (kaldet SaaS-specifikke produktvilkår) og dokumentet IBM Vilkår for brug – Standardvilkår (kaldet Standardvilkår), som er tilgængeligt på adressen http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

I tilfælde af en uoverensstemmelse har de SaaS-specifikke produktvilkår forrang for Standardvilkårene. Ved at bestille, tilgå eller benytte IBM SaaS-produktet accepterer Kunden disse Vilkår for brug.

Disse Vilkår for brug er reguleret af IBM International Passport Advantage-Aftalen, IBM International Passport Advantage Express-Aftalen eller IBM International Aftale om Udvalgte IBM SaaS-produkter (hver især kaldet Aftalen), som sammen med Vilkår for brug udgør den fuldstændige aftale.

1. IBM SaaS

De SaaS-specifikke produktvilkår dækker følgende IBM SaaS-produkter:

1.1 IBM SaaS Rapport-produkter

- 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 IBM SaaS Pinpoint-produkter

- 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 Mobile IBM SaaS-produkter

- 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. Måletyper for betaling

IBM SaaS-produktet sælges og betales på basis af en af følgende målinger, som angivet i Transaktionsdokumentet:

a. **Kvalificeret Deltager (Eligible Participant)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Enhver enkeltperson eller enhed, som er kvalificeret til at deltage i et serviceleveringsprogram, der administreres eller spores af IBM SaaS-produktet, er Kvalificeret Deltager. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække det samlede antal Kvalificerede Deltagere, som administreres eller spores i IBM SaaS-produktet i den måleperiode, der er angivet i Kundens Transaktionsdokument.

   De enkelte serviceleveringsprogrammer, der administreres af IBM SaaS-produktet, analyseres separat, og resultaterne lægges derefter sammen. Enkeltpersoner eller enheder, der er kvalificeret til flere serviceleveringsprogrammer, kræver separate brugsrettigheder.

   I disse produkter omfatter et serviceleveringsprogram en enkelt Business- eller Retail-applikation fra Kunden med en logonstartside og tilhørende sider for hver Business- eller Retail-applikation. En Kvalificeret Deltager er en slutbruger hos en Kunde, som har logon-rettigheder til en Business- eller Retail-applikation.

b. **Client-enhed (Client Device)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. En Client-enhed er en enkelt brugers IT-enhed, en sensor til et specielt formål eller en telemetrienhed, som anmoder om gennemførelse af eller modtager – med henblik på udførelse – et sæt kommandoer, procedurer eller applikationer fra, eller leverer data til, et andet computersystem, der typisk kaldes en server, eller som administreres af serveren. Flere Client-enheder kan være fælles om adgangen til en server. En Client-enhed kan have en vis databehandlingskapacitet eller kan programmeres, så en bruger kan arbejde på den. Kunden skal anskaffe brugsrettigheder til hver enkelt Client-enhed, der kører, leverer data til, bruger ydelser leveret af eller på anden måde har adgang til IBM SaaS-produktet i den måleperiode, som er angivet i Kundens Transaktionsdokument.

3. Pris og fakturering

Det beløb, der skal betales for IBM SaaS-produktet, er angivet i et Transaktionsdokument.

3.1 Betaling for del af måned

Betaling for en del af en måned, som angivet i Transaktionsdokumentet, kan opgøres forholdsvist.

4. Regeloverholdelse og revision

Adgang til IBM Security Trusteer Fraud Protection-produkterne er begrænset til et maksimalt antal Kvalificerede Deltagere eller Client-enheder som angivet i Transaktionsdokumentet. Kunden har ansvaret for at sikre, at Kundens antal Kvalificerede Deltagere eller Client-enheder ikke overstiger det maksimale antal, som er angivet i Transaktionsdokumentet.

Der kan udføres en revision for at kontrollere, at det maksimale antal Kvalificerede Deltagere eller Client-enheder ikke overskrides.

5. Fornyelse af IBM SaaS-abonnementsperioden

Kundens Transaktionsdokument angiver, om IBM SaaS-produktet fornys ved Abonnementsperiodens udløb. En af følgende er angivet:

5.1 Automatisk fornyelse

Hvis Kundens Transaktionsdokument angiver, at fornyelsen sker automatisk, kan Kunden opsige den IBM SaaS-abonnementsperiode, der udløber, via skriftlig anmodning til Kundens IBM-konsulent eller IBM Business Partner mindst 90 dage inden udløbsdatoen, som er angivet i Transaktionsdokumentet. Hvis IBM eller Kundens IBM Business Partner ikke modtager en sådan anmodning senest på udløbsdatoen, bliver Abonnementsperioden automatisk fornyet med ét år eller med samme varighed, som den oprindelige Abonnementsperiode, der er angivet i Transaktionsdokumentet.

5.2 Løbende fakturering

Hvis der i Transaktionsdokumentet står, at fornyelse sker løbende, har Kunden fortsat adgang til IBM SaaS-produktet og vil løbende blive faktureret for brug af IBM SaaS-produktet. Hvis Kunden ikke længere vil bruge IBM SaaS-produktet og ønsker at standse den løbende fakturering, skal Kunden med 90 dages skriftligt varsel til IBM eller Kundens IBM Business Partner anmode om, at Kundens IBM SaaS-produkt bliver annulleret. Når Kundens adgang annulleres, bliver Kunden faktureret for eventuelle udestående betalinger for adgang til og med den måned, hvor annulleringen trådte i kraft.

5.3 Fornyelse påkrævet

Hvis der i Transaktionsdokumentet står, at Kundens brug af IBM SaaS-produktet ophører på fornyelsestidspunket, ophører IBM SaaS-produktet ved udgangen af Abonnementsperioden, og Kundens adgang til IBM SaaS-produktet fjernes. Hvis Kunden vil bruge IBM SaaS-produktet efter udløbsdatoen, skal Kunden afgive en ordre hos IBM's salgskonsulent eller en IBM Business Partner om køb af en ny Abonnementsperiode.

6. Teknisk support

Der er inkluderet teknisk support til IBM SaaS-produktet for Kunden og dennes Kvalificerede Deltagere som hjælp til brugen af IBM SaaS-produktet.

Abonnementet på hvert produkt omfatter Standardsupport. Trusteer Rapport Mandatory Service, der er en tillægsydelse til Trusteer Rapport, forudsætter Premium-support til basisabonnementet på Trusteer Rapport.

Til hvert IBM SaaS-produkt findes der et Premium-supportabonnement, som kan anskaffes mod ekstra betaling, med undtagelse af IBM Security Trusteer Mobile SDK-produkter og IBM Security Trusteer Rapport Mandatory Service-produkter.

Standardsupport:

- 8.00-17.00 lokal tid.
- Kunderne og deres Kvalificerede Deltagere kan sende problemrapporter elektronisk som beskrevet i håndbogen Software as a Service [SaaS] Support Handbook.
- Via kundesupportportalen kan Kunderne få adgang til meddelelser, dokumenter, sagsrapporter og ofte stillede spørgsmål på: http://www-01.ibm.com/software/security/trusteer/support/.
- Der er flere oplysninger om supportmuligheder og flere detaljer i håndbogen IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

Premium-support:

- Support 24x7 for alle problemklassificeringskoder.
- Kunderne kan kontakte support direkte via telefon.
- Kunderne og deres Kvalificerede Deltagere kan sende problemrapporter elektronisk som beskrevet i håndbogen Software as a Service [SaaS] Support Handbook.
- Via kundesupportportalen kan Kunderne få adgang til meddelelser, dokumenter, sagsrapporter og ofte stillede spørgsmål på: http://www-01.ibm.com/software/security/trusteer/support/.
- Der er flere oplysninger om supportmuligheder og flere detaljer i håndbogen IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

7. Tillægsvilkår for IBM SaaS

7.1 Overholdelse af Safe Harbor-principperne

IBM overholder principperne i Safe Harbor-ordningen, som er aftalt mellem USA og EU og udviklet af det amerikanske handelsministerium i samarbejde med Europa-Kommissionen. IBM Security Trusteer-produkter er omfattet af IBM's certificering under Safe Harbor-ordningen mellem EU og USA. Der er flere oplysninger om Safe Harbor-ordningen og en liste med virksomheder, som er inkluderet i Safe Harbor-ordningen, på http://export.gov/safeharbor/.

7.2 Forhøjelse af Kundens årlige abonnementsgebyr

IBM forbeholder sig ret til at ændre abonnementsgebyret for IBM SaaS-produktet højst én gang hver 12. måned med en procentsats, der fastlægges af IBM, og som ikke overstiger 3 %. Ændringen i abonnementsgebyret træder i kraft på årsdagen for startdatoen for den første dækningsperiode. Denne gebyrændring ændrer ikke ved Kundens brugsrettigheder til IBM SaaS-produktet eller den måletype for betaling, som IBM SaaS-produktet er anskaffet på basis af. IBM Business Partnere er uafhængige af IBM og fastlægger selv deres priser og vilkår.

7.3 Premium-support

Kunden er kun berettiget til Premium-support til IBM SaaS-produkter, hvor Kunden abonnerer på det tilknyttede Premium Support-produkt.

7.4 Retmæssig brug og samtykke

Bemyndigelse til at indsamle og behandle data

IBM SaaS-produktet har til formål at hjælpe Kunden med at forbedre sit sikkerhedsmiljø og sine data. IBM SaaS-produktet indsamler oplysninger fra Kvalificerede Deltagere og Client-enheder, der interagerer med de Business- og Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til. IBM SaaS-produktet indsamler oplysninger, der alene eller samlet kan anses for personoplysninger i nogle jurisdiktioner. Personoplysninger er oplysninger, der kan bruges til at identificere en bestemt person, for eksempel et navn, en e-mail-adresse, hjemadresse eller et telefonnummer, og som leveres til IBM med det formål at opbevare, behandle eller overføre oplysningerne på Kundens vegne.

Dataindsamling og databehandlingspraksis kan blive opdateret for at forbedre funktionaliteten i IBM SaaS-produktet. Et dokument med en fuld beskrivelse af dataindsamlingen og databehandlingspraksis opdateres efter behov og er efter anmodning tilgængeligt for Kunden. Kunden bemyndiger IBM til at indsamle disse oplysninger og behandle dem i overensstemmelse med afsnittene Overførsel på tværs af grænser og Databeskyttelse og datasikkerhed i standardvilkårene i Vilkår for brug.

Vedrørende IBM Security Trusteer Pinpoint-produkter:

Indsamlede data kan omfatte brugerens IP-adresse, krypteret bruger-id eller bruger-id med envejs-hash-værdi, domænecookier, hvis de ikke er filtreret fra, besøg i beskyttede applikationer og på phishing-sider, geografisk placering samt brugeroplysninger, der angives på phishing-sider.

Vedrørende IBM Security Trusteer Mobile SDK-proodukter og IBM Security Trusteer Mobile Browser-produkter:

Indsamlede data kan omfatte brugerens IP-adresse, krypteret bruger-id eller bruger-id med envejs-hash-værdi, geografisk lokalitet og besøg i beskyttede applikationer, SIM-kortoplysninger, enhedsnavn samt kundetilhørsforhold.

Vedrørende IBM Security Trusteer Rapport-produkter:

Indsamlede data kan omfatte brugerens IP-adresse, krypteret bruger-id eller bruger-id med envejs-hash-værdi, sikkerhedsbegivenheder, brugernavn og e-mailadresse, der er opgivet til IBM med henblik på kundesupport, kundetilhørsforhold, krypteret kodeord, der angives på beskyttede sider, besøg i beskyttede applikationer og på phishing-sider, krypteret betalingskortnummer samt filer og data indsamlet eksternt af IBM-medarbejdere med henblik på undersøgelse af formodet malware, ondartede aktiviteter eller fejl.

Informeret samtykke fra registrerede personer:

Brugen af dette IBM SaaS-produkt kan være underlagt forskellige love eller regler. IBM SaaS-produktet må kun anvendes til lovlige formål og på lovlig vis. Kunden erklærer sig indforstået med at anvende IBM SaaS-produktet i henhold til relevante love, regler og politikker og påtager sig ethvert ansvar for at overholde disse.

Vedrørende IBM Security Trusteer Pinpoint-produkter og IBM Security Trusteer Mobile SDK-produkter:

Kunden bekræfter, at Kunden har indhentet eller vil indhente alle fuldt informerede samtykker, tilladelser eller licenser, der er nødvendige for at kunne bruge IBM SaaS-produktet på lovlig vis, og som tillader IBM at indsamle og behandle oplysninger via IBM SaaS-produktet.

Vedrørende IBM Security Trusteer Rapport-produkter og IBM Security Trusteer Mobile Browser-produkter:

Kunden bemyndiger IBM til at indhente de fuldt informerede samtykker, der er nødvendige for at muliggøre lovlig brug af IBM SaaS-produktet og for at indsamle og behandle oplysninger som beskrevet i slutbrugerlicensaftalen, der kan ses på https://www.trusteer.com/support/end-user-license-agreement. Såfremt Kunden beslutter, at Kunden (og ikke IBM) skal stå for kommunikationen med slutbrugere vedrørende samtykke, bekræfter Kunden, at Kunden har indhentet eller vil indhente alle fuldt informerede samtykker, tilladelser eller licenser, der er nødvendige for at kunne bruge IBM SaaS-produktet på lovlig vis, og som tillader IBM som Kundens databehandler at indsamle og behandle oplysningerne via IBM SaaS-produktet.

7.5 Overførsel på tværs af grænser

Kunden giver samtykke til, at IBM må behandle Indhold, herunder eventuelle Personoplysninger, i henhold til relevante love og krav på tværs af landegrænser til databehandlere og underdatabehandlere i følgende lande uden for Det Europæiske Økonomiske Samarbejdsområde og lande, der af Europa-Kommissionen anses for at have et tilstrækkeligt sikkerhedsniveau: USA.

7.6 Datasikkerhed

Hvis Kunden gør Personoplysninger tilgængelige for IBM SaaS i EU's medlemsstater, Island, Liechtenstein, Norge eller Schweiz, eller hvis Kunden har Kvalificerede Deltagere eller Client-enheder i disse lande, udpeger Kunden som fuldt dataansvarlig IBM som databehandler (som disse udtryk er defineret som henholdsvis "registeransvarlig" og "registerfører" i EU-direktiv 95/46/EF) til at behandle Personoplysninger. IBM behandler kun sådanne Personoplysninger i det omfang, det er nødvendigt for at gøre IBM SaaS-produktet tilgængeligt i overensstemmelse med IBM's offentliggjorte beskrivelser af IBM SaaS, og Kunden er indforstået med, at enhver sådan behandling er i overensstemmelse med Kundens anvisninger. IBM giver Kunden er rimeligt varsel, hvis IBM foretager en væsentlig ændring med hensyn til behandlingssted eller den måde, IBM sikrer Personoplysninger på som del af IBM SaaS. Kunden kan opsige den aktuelle Abonnementsperiode, for så vidt angår det berørte IBM SaaS-produkt, ved at give IBM skriftlig besked senest 30 dage efter, at IBM har informeret Kunden om ændringen. Kunden giver samtykke til, at IBM må behandle Indhold, herunder Personoplysninger, på tværs af landegrænser til følgende databehandlere og underdatabehandlere:

Navn på databehandler/ underdatabehandler	Rolle (databehandler eller underdatabehandler)	Sted*
Kontraherende IBM-enhed	Databehandler	Som angivet i Transaktionsdokumentet
Amazon Web Services LLC	Underdatabehandler	410 Terry Ave. N Seattle, WA 98109 USA

Navn på databehandler/ underdatabehandler	Rolle (databehandler eller underdatabehandler)	Sted*
Connectria Corp.	Underdatabehandler	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 USA
IBM Israel Ltd.	Underdatabehandler	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Underdatabehandler	1 New Orchard Rd. Armonk, NY 10504 USA

Kunden accepterer, at IBM med et varsel kan ændre landelisten, hvis IBM med rimelighed beslutter, det er nødvendigt for leveringen af IBM SaaS-produktet.

Kunden er indforstået med, at for en serviceydelse, der leveres via det tyske datacenter, som angivet i forbindelse med klargøringen, må IBM behandle Indhold, herunder Personoplysninger, på tværs af landegrænser til følgende databehandlere og underdatabehandlere:

Navn på databehandler/ underdatabehandler	Rolle (databehandler eller underdatabehandler)	Sted*
Kontraherende IBM-enhed	Databehandler	Som angivet i Transaktionsdokumentet
Amazon Web Services (Germany)	Underdatabehandler	München, Tyskland
IBM Israel Ltd.	Underdatabehandler	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Kunden er indforstået med, at for en serviceydelse, der leveres via det japanske datacenter, som angivet i forbindelse med klargøringen, må IBM behandle Indhold, herunder Personoplysninger, på tværs af landegrænser til følgende databehandlere og underdatabehandlere:

Navn på databehandler/ underdatabehandler	Rolle (databehandler eller underdatabehandler)	Sted*
Kontraherende IBM-enhed	Databehandler	Som angivet i Transaktionsdokumentet
Amazon Web Services (Japan)	Underdatabehandler	Tokyo, Japan
IBM Israel Ltd.	Underdatabehandler	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* De steder, der er angivet i tabellerne ovenfor, inkluderer adresserne på Databehandlerens/Underdatabehandlerens hovedkontor. Datacentrene befinder sig i det samme land.

Parterne eller deres relevante associerede eller koncernforbundne virksomheder kan indgå separate aftaler ved brug af EU's uændrede standardaftaler i deres aktuelle roller i henhold til EU-beslutning 2010/87/EU, hvor de valgfri betingelser er fjernet. Parterne skal behandle enhver uenighed eller forpligtelse, som opstår i forbindelse med disse aftaler – også selvom aftalen er indgået af en associeret eller koncernforbunden virksomhed – som om uenigheden eller forpligtelsen er opstået mellem parterne under vilkårene i denne Aftale.

Bilag A

1. IBM SaaS-produkter

IBM tilbyder disse serviceydelser som enkeltstående serviceydelser og produkter eller som tillægsydelser og -produkter. De specifikke IBM SaaS-produkter, der er bestilt, er angivet i Kundens bevis for brugsret.

1.1 Business- og Retail-definitioner

IBM Security Trusteer Fraud-produkter er licenseret til brug sammen med bestemte typer applikationer. En Applikation er defineret som en af følgende typer: Retail eller Business. Der findes forskellige produkter til Retail-applikationer og Business-applikationer.

- En Retail-applikation er defineret som en netbankapplikation, mobilapplikation eller e-handelsapplikation, der har til formål at servicere forbrugere. Kundens politik kan klassificere visse mindre virksomheder som værende kvalificerede til adgang til Retail-produkter.
- En Business-applikation er defineret som en netbankapplikation, mobilapplikation eller e-handelsapplikation, der har til formål at servicere virksomheder, organisationer og lignende, eller enhver applikation, der ikke er kategoriseret som en Retail-applikation.

1.2 IBM SaaS-produkter med basisabonnement

Business-produkter:

- 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

Retail-produkter:

- 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

Til hvert Business- eller Retail-produkt findes der et tilknyttet Premium Support-produkt, som kan anskaffes mod ekstra betaling, med undtagelse af IBM Security Trusteer Mobile SDK-produkter.

1.3 IBM SaaS-tillægsabonnementer til IBM Security Trusteer Rapport-produkter

Tillægsprodukter til IBM Security Trusteer Rapport for Business:

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

Tillægsprodukter til IBM Security Trusteer Rapport for Retail:

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

Til hvert Business- og Retail-tillægsprodukt til IBM Security Trusteer Rapport-produkter, med undtagelse af IBM Security Trusteer Rapport Mandatory Service-tillægsprodukter, findes der et tilknyttet Premium Support-produkt, som kan anskaffes mod ekstra betaling.

Et abonnement på IBM Security Trusteer Rapport for Business eller IBM Security Trusteer Rapport for Retail er en forudsætning for de tilknyttede IBM SaaS-tillægsabonnementer, der er angivet i dette afsnit.

1.4 IBM SaaS-tillægsabonnementer til IBM Security Trusteer Pinpoint Malware Detection-produkter

Tillægsprodukter til IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition eller IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Tillægsprodukter til IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition eller 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

Et Premium Support-abonnement fås – mod betaling af et ekstra gebyr – til hvert af de IBM SaaS-tillægsprodukter, der er angivet i dette afsnit.

Et abonnement på IBM Security Trusteer Pinpoint Malware Detection for Business-produkter eller IBM Security Trusteer Pinpoint Malware Detection for Retail-produkter er en forudsætning for de tilknyttede IBM SaaS-tillægsabonnementer, der er angivet i dette afsnit.

1.5 Andre IBM SaaS-tillægsabonnementer

De eventuelle IBM SaaS-tillægsabonnementer til ovenstående basisabonnementer, der ikke er angivet her, hvad enten de er tilgængelige på nuværende tidspunkt eller er under udvikling, anses ikke for at være opdateringer og skal tildeles separat.

1.6 Definitioner

Kontohaver – betyder den slutbruger hos Kunden, som har installeret klientaktiveringssoftwaren, accepteret slutbrugerlicensaftalen ("EULA") og mindst én gang er logget på Kundens Retail- eller Business-applikation, som Kunden abonnerer på IBM SaaS-dækning til.

Kontohaver-Klientsoftware – betyder IBM Security Trusteer Rapport-klientaktiveringssoftware eller IBM Security Trusteer Mobile Browser-klientaktiveringssoftware eller enhver anden klientaktiveringssoftware, der leveres sammen med nogle IBM SaaS-abonnementer til installation på slutbrugerens enhed.

Målside – refererer til den side, der hostes af IBM, og som leveres til Kunden med kunde-splash og Kontohaver-Klientsoftware til downloadning.

Trusteer Splash – refererer til den splash, der leveres til Kunden på basis af tilgængelige splash-skabeloner.

2. IBM Security Trusteer Rapport-produkter

2.1 IBM Security Trusteer Rapport for Retail og/eller IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport tilbyder et lag af beskyttelse mod phishing og MitB-malwareangreb (Man-in-the-Browser). Via et netværk af millioner af slutpunkter på hele kloden indsamler IBM Security Trusteer Rapport oplysninger om aktive phishing- og malwareangreb mod virksomheder verden over. IBM Security Trusteer Rapport anvender adfærdsalgoritmer, der har til formål at blokere phishing-angreb og hindre, at MitB-malwarevirusser bliver installeret og fungerer.

Dette IBM SaaS-produkt har betalingsmåletypen Kvalificeret Deltager. Business-produktet sælges i pakker med 10 Kvalificerede Deltagere. Retail-produktet sælges i pakker af 100 Kvalificerede Deltagere.

Dette IBM SaaS-produkt inkluderer:

a. Trusteer Management Application ("TMA"):

   Der er adgang til TMA i det cloud-hostede IBM Security Trusteer-miljø, hvor Kunden (og et ubegrænset antal medarbejdere med relevant tilladelse) kan: (i) modtage begivenhedsdatarapportering og risikovurderinger, (ii) få vist, konfigurere og fastlægge regler vedrørende rapportering af begivenhedsdata samt (iii) få vist konfiguration af klientaktiveringssoftwaren, der er licenseret uden omkostninger til offentligheden i henhold til en slutbrugerlicensaftale ("EULA"), og som kan downloades til den Kvalificerede Deltagers computere eller enheder (pc/Mac), også kendt som Trusteer Rapport-softwarepakken ("Kontohaver-Klientsoftware"). Kunden må kun markedsføre Kontohaver-Klientsoftware via Trusteer Splash- eller Rapport-API'en, og Kunden må ikke anvende Kontohaver-Klientsoftware til sine interne forretningsaktiviteter eller til sine medarbejderes brug (ud over medarbejdernes personlige brug).

b. Webscript:

   Til installation på et websted med det formål at få adgang til eller bruge IBM SaaS-produkterne.

c. Begivenhedsdata:

   Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage begivenhedsdata, der er genereret via Kontohaver-Klientsoftware som resultat af Kontohavers onlineinteraktioner med sin Business- eller Retail-applikation, som Kunden abonnerer på IBM SaaS-dækning til. Begivenhedsdata modtages fra de Kvalificerede Deltageres Kontohaver-Klientsoftware, som kører på enheder hos dem, der har accepteret EULA-aftalen ved at logge på Kundens Business- eller Retail-applikation mindst én gang, og Kundens konfiguration skal omfatte indsamling af bruger-id'er.

d. Trusteer Splash:

   Trusteer Splash-markedsføringsplatformen identificerer og markedsfører Kontohaver-Klientsoftware til de Kvalificerede Deltagere, der logger på Kundens Business- og/eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til. Kunden kan vælge mellem de tilgængelige Splash-skabeloner. Tilpasset splash kan arrangeres via en separat aftale eller servicebeskrivelse.

Kunden kan erklære sig indforstået med at levere sine varemærker, logoer eller ikoner til brug i forbindelse med TMA og kun til benyttelse sammen med Trusteer Splash samt til visning i Kontohaver-Klientsoftware eller på den målside, der hostes af IBM, og på IBM Security Trusteer-webstedet. Enhver brug af de leverede varemærker, logoer eller ikoner vil ske i henhold til IBM's relevante regler vedrørende reklame og brug af varemærker.

Kunden skal abonnere på IBM Security Trusteer Rapport Mandatory Service SaaS-produktet, hvis Kunden ønsker at anvende en hvilken som helst type obligatorisk implementering af Kontohaver-Klientsoftware.

Obligatorisk implementering af Kontohaver-Klientsoftware omfatter f.eks. enhver type obligatorisk implementering via en mekanisme eller et middel, der direkte eller indirekte tvinger en Kvalificeret Deltager til at downloade Kontohaver-Klientsoftware, eller en metode, et værktøj, en procedure, aftale eller mekanisme, som ikke er oprettet eller godkendt af IBM, og som er oprettet for at omgå licenskravene for denne obligatoriske implementering af Kontohaver-Klientsoftware.

2.2 Valgfrie IBM SaaS-tillægsprodukter til IBM Security Trusteer Rapport for Business og/eller IBM Security Trusteer Rapport for Retail

Et abonnement på IBM Security Trusteer Rapport-produkter er en forudsætning for at kunne abonnere på et eller flere af de følgende IBM SaaS-tillægsprodukter. Hvis IBM SaaS-produktet er markeret som "for Business", skal det anskaffede IBM SaaS-tillægsprodukt også være markeret som "for Business". Hvis IBM SaaS-produktet er markeret som "for Retail", skal det anskaffede IBM SaaS-tillægsprodukt også være markeret som "for Retail". Kunden modtager begivenhedsdata fra de Kvalificerede Deltagere, der kører Kontohaver-Klientsoftware, og som har accepteret EULA-aftalen ved at logge på Kundens Business- eller Retail-applikation mindst én gang, og Kundens konfiguration skal omfatte indsamling af bruger-id'er.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business og/eller IBM Security Trusteer Rapport Fraud Feeds for Retail

Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage begivenhedsdata vedrørende malwareangreb og andre slutpunktssårbarheder på en bestemt Kontohavers skrivebord.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business og/eller IBM Security Trusteer Rapport Phishing Protection for Retail

Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage meddelelser om begivenhedsdata, som er knyttet til videresendelse af Kontohavers brugeroplysninger til en formodet phishingside eller en potentielt svigagtig side. Lovlige onlineapplikationer (url-adresser) kan fejlagtigt blive markeret som phishingsider, og IBM SaaS-produktet kan advare Kontohavere om, at en lovlig side er en phishingside. I så fald skal Kunden underrette IBM om fejlen, og IBM skal rette fejlen. Dette udgør Kundens eneste retsmiddel ved en sådan fejl.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business og/eller IBM Security Trusteer Rapport Mandatory Service for Retail

Kunden kan bruge en forekomst af Trusteer Splash-markedsføringsplatformen til at tillade downloadning af Kontohaver-Klientsoftware til Kvalificerede Deltagere, der bruger Kundens Business- og/eller Retail-applikation, som Kunden abonnerer på IBM SaaS-dækning til.

IBM Security Trusteer Rapport Premium Support for Business er en forudsætning for IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail er en forudsætning for IBM Security Rapport Mandatory Service for Retail.

Kunden kan kun implementere IBM Security Trusteer Rapport Mandatory Service-tillægsfunktionalitet, hvis den blev bestilt og konfigureret til brug sammen med Kundens Retail- eller Business-applikation, som Kunden abonnerer på IBM SaaS-dækning til.

3. IBM Security Trusteer Pinpoint-produkter

IBM Security Trusteer Pinpoint er en cloud-baseret serviceydelse, der er designet til at give endnu et lag af beskyttelse, og som har til formål at spore og modvirke malware, phishing og forsøg på kontoovertagelse. Trusteer Pinpoint kan integreres med de af Kundens Business- og/eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til, og med processer til forebyggelse af svindel.

Dette IBM SaaS-produkt inkluderer:

a. TMA:

   Der er adgang til TMA i det cloud-hostede IBM Security Trusteer-miljø, hvor Kunden (og et ubegrænset antal medarbejdere med relevant tilladelse) kan: (i) modtage begivenhedsdatarapportering og risikovurderinger, (ii) få vist, konfigurere og fastlægge sikkerhedsregler og regler vedrørende rapportering af begivenhedsdata.

b. Webscript og/eller API'er:

   Til installation på et websted med det formål at få adgang til eller bruge IBM SaaS-produktet.

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

Ved sporing af malware i IBM Security Trusteer Pinpoint Malware Detection-produkter eller ved registrering af kontoovertagelse i IBM Security Trusteer Pinpoint Criminal Detection-produkter skal Kunden følge vejledningen i Pinpoint Best Practices Guide. IBM Security Trusteer Pinpoint Malware Detection-produkter eller IBM Security Trusteer Pinpoint Criminal Detection-produkter må ikke anvendes på en måde, der kan påvirke den Kvalificerede Deltagers oplevelse umiddelbart efter registrering af malware eller kontoovertagelse, således at andre ville være i stand til at knytte Kundens handlinger til brugen af IBM Security Trusteer Pinpoint-produkter (f.eks. meddelelser, beskeder, blokering af enheder eller blokering af adgang til Business- og/eller Retail-applikationen umiddelbart efter registrering af malware eller kontoovertagelse).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business og/eller IBM Security Trusteer Pinpoint Criminal Detection for Retail

Klientløs sporing af en mistænkelig kontoovertagelsesaktivitet i browsere, der har forbindelse til en Business- eller Retail-applikation, ved hjælp af enheds-id, sporing af phishing og sporing af malware-baseret tyveri af brugeroplysninger. IBM Security Trusteer Pinpoint Criminal Detection-produkter tilbyder et ekstra lag af beskyttelse og har til formål at spore kontoovertagelsesforsøg og levere risikovurdering af browsere eller mobile enheder (via den indbyggede browser eller Kundens mobilapplikation), som har adgang til en Business- eller Retail-applikation, direkte til Kunden.

a. Begivenhedsdata:

   Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage begivenhedsdata, der genereres som følge af Kvalificerede Deltageres onlineinteraktioner med Kundens Business- og/eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til, eller Kunden kan modtage begivenhedsdata via en backend-API-leverancetilstand.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile og/eller IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

IBM Security Trusteer Pinpoint Criminal Detection for Mobile-produkter (PPCD Mobile) er designet til at give et ekstra lag af beskyttelse og har til formål at beskytte mod kontoovertagelse og svigagtige aktiviteter ved at identificere kriminel kontoadgang og via generering af en anbefaling til Kunden. Dette IBM SaaS-produkt indsamler oplysninger både fra Kundens Business- og/eller Retail-applikation ved hjælp af PPCD Mobile-API'en og fra Kvalificerede Deltageres mobilenheder. IBM Security Trusteer PPCD Mobile-produkter er designet til at sammenholde komplekse oplysninger om Kvalificerede Deltageres mobilenheder med data fra andre datakilder, f.eks. oplysninger om malwareinfektion og phishing-hændelser i realtid, som integreres via IBM Security Trusteers andre IBM SaaS-produkter, der er angivet i disse Vilkår for brug.

Kunden kan få adgang til og bruge IBM Security Trusteer PPCD Mobile-produkterne i IBM Security Trusteers cloud-hostede miljø og modtage risikovurderingsoplysninger fra Kvalificerede Deltageres mobilenheder, genereret som resultat af disse mobilenheders onlineinteraktioner med Kundens Business- eller Retail-applikation, som Kunden abonnerer på IBM SaaS-dækning til. I forbindelse med disse produkter omfatter "mobilenheder" kun understøttede mobiltelefoner og tablets og ikke bærbare computere eller Mac-computere.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Klientløs sporing af browsere, der er angrebet af finansiel MitB-malware (Man-in-the-Browser), og som har forbindelse til en Business- og/eller Retail-applikation. IBM Security Trusteer Pinpoint Malware Detection-produkter tilbyder et ekstra lag af beskyttelse og har til formål at sætte virksomheder i stand til at fokusere på processer til forebyggelse af svindel baseret på risikoen for malware. Det sker ved at give Kunden vurderinger og advarsler om tilstedeværelsen af finansiel MitB-malware.

a. Begivenhedsdata:

   Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage begivenhedsdata, der genereres som følge af Kvalificerede Deltageres onlineinteraktioner med Kundens Business- og/eller Retail-applikation(er).

b. Advanced Edition:

   Advanced Edition for Business og/eller for Retail tilbyder et ekstra lag af sporing og beskyttelse, som justeres og tilpasses Kundens Business- og/eller Retail-applikationers struktur og arbejdsgang. Det kan også tilpasses det specifikke trusselsbillede, der er rettet mod Kunden. Det kan indbygges forskellige steder i Kundens Business- og/eller Retail-applikationer.

   Advanced Edition tilbydes Kunden i en minimumsantal på 100.000 Kvalificerede Deltagere for Retail eller 10.000 Kvalificerede Deltagere for Business. Det svarer til 1000 pakker med 100 Kvalificerede Deltagere for Retail eller 1000 pakker med 10 Kvalificerede Deltagere for Business.

c. Standard Edition:

Standard Edition for Business eller for Retail er en løsning, der er hurtig at implementere, og som indeholder IBM SaaS-produktets kernefunktionalitet som beskrevet heri.

3.2 Valgfrie IBM SaaS-tillægsprodukter til IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition og/eller IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

IBM Security Trusteer Rapport Remediation for Retail-produkter forudsætter IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

IBM Security Trusteer Pinpoint Carbon Copy for Retail forudsætter IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. IBM Security Trusteer Pinpoint Carbon Copy for Business forudsætter IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business og/eller IBM Security Trusteer Pinpoint Carbon Copy for Retail

IBM Security Trusteer Pinpoint Carbon Copy-produkter er designet til at give et ekstra lag af beskyttelse og tilbyde en overvågningsservice, som kan bidrage til at klarlægge, hvornår en Kvalificeret Deltagers brugeroplysninger er blevet kompromitteret af phishingangreb på Kundens Retail- eller Business-applikationer, som Kunden abonnerer på IBM SaaS-dækning til.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail har til formål at undersøge, afhjælpe, blokere og fjerne MitB-malwareinfektioner (Man in the Browser) fra inficeret udstyr (pc/Mac) hos de af Kundens Kvalificerede Deltagere, der har adgang til Kundens Retail-applikation på ad hoc-basis, hvor MitB-malwareinfektioner er blevet sporet af IBM Security Trusteer Pinpoint Malware Detection-begivenhedsdata. Kunden skal have et gyldigt abonnement på IBM Security Trusteer Pinpoint Malware Detection, som faktisk kører på Kundens Retail-applikation. Kunden må kun bruge dette IBM SaaS-produkt i forbindelse med Kvalificerede Deltagere, der logger på Kundens Retail-applikation, og udelukkende som et værktøj til at undersøge og afhjælpe en bestemt inficeret enhed (pc/Mac) på ad hoc-basis. IBM Security Trusteer Rapport Remediation for Retail skal faktisk køre på en sådan Kvalificeret Deltagers inficerede enhed (pc/Mac), og en sådan berørt Kvalificeret Deltager skal acceptere EULA-aftalen ved at logge på Kundens Retail-applikation(er) mindst én gang, og Kundens konfiguration skal omfatte indsamling af bruger-id'er. Dette IBM SaaS-produkt omfatter ikke retten til at bruge Trusteer Splash og/eller til på anden måde generelt at markedsføre Kontohaver-Klientsoftware over for Kundens gruppe af Kvalificerede Deltagere.

4. IBM Security Trusteer Mobile-produkter

4.1 IBM Security Trusteer Mobile Browser for Business og/eller IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser er designet til at give et ekstra lag af beskyttelse og har til formål at tilbyde sikker onlineadgang for Kvalificerede Deltageres mobile enheder, der har adgang til de af Kundens Retail- eller Business-applikationer, som Kunden abonnerer på IBM SaaS-dækning til, samt tilbyde risikovurdering af mobile enheder og beskyttelse mod phishing. Sikker Wi-Fi-sporing findes kun til Android-platforme. Derfor omfatter dette IBM SaaS-produkt mobile enheder såsom mobiltelefoner eller tablets, men ikke bærbare computere og Mac-computere.

Via TMA kan Kunden (og et ubegrænset antal medarbejdere med relevant tilladelse) modtage begivenhedsdata, analyser og statistiske oplysninger, som er knyttet til enheder, der tilhører Kvalificerede Deltagere, som har: (i) downloadet Kontohaver-Klientsoftware, en applikation, der vederlagsfrit er alment licenseret i henhold til en slutbrugerlicensaftale ("EULA"), og som kan downloades til de Kvalificerede Deltageres mobile enheder, og (ii) accepteret EULA-aftalen og mindst én gang er logget på de af Kundens Business- eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til. Kunden må kun markedsføre Kontohaver-Klientsoftware via Trusteer Splash og må ikke anvende Kontohaver-Klientsoftware til sine interne forretningsaktiviteter.

a. Begivenhedsdata:

Kunden (og et ubegrænset antal af Kundens medarbejdere med relevant tilladelse) kan bruge TMA til at modtage begivenhedsdata, der er genereret som følge af mobilenhedernes onlineinteraktioner med Kundens Retail- eller Business-applikationer, som Kunden abonnerer på IBM SaaS-dækning til.

b. Trusteer Splash:

Trusteer Splash-markedsføringsplatformen identificerer og markedsfører Kontohaver-Klientsoftware til de Kvalificerede Deltagere, der logger på Kundens Business- og/eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til. Kunden kan vælge mellem de tilgængelige Splash-skabeloner ("Splash-skabelon"). Tilpasset splash kan arrangeres via en separat aftale eller servicebeskrivelse.

Kunden kan erklære sig indforstået med at levere sine varemærker, logoer eller ikoner til brug i forbindelse med TMA og kun til benyttelse sammen med Trusteer Splash samt til visning i Kontohaver-Klientsoftware eller på den målside, der hostes af IBM, eller på IBM Security Trusteer-webstedet. Enhver brug af de leverede varemærker, logoer eller ikoner vil ske i henhold til IBM's relevante regler vedrørende reklame og brug af varemærker.

4.2 IBM Security Trusteer Mobile SDK for Business og/eller IBM Security Trusteer Mobile SDK for Retail

IBM Security Trusteer Mobile SDK-produkter er designet til at give et ekstra lag af beskyttelse og sørge for sikker webadgang til Business- og/eller Retail-applikationer, som Kunden abonnerer på IBM SaaS-dækning til, samt sørge for risikovurdering af enheder og beskyttelse mod pharming. Sikker Wi-Fi-sporing findes kun til Android-platforme.

IBM Security Trusteer Mobile SDK-produkter omfatter en retsligt beskyttet Mobile Software Developer's Kit ("SDK"), som er en softwarepakke med dokumentation, retsligt beskyttede softwareprogrammeringsbiblioteker og andre tilknyttede filer og elementer, kendt som IBM Security Trusteer Mobile Library, samt "Runtime-komponenten" eller "den Redistribuérbare komponent", som er en retsligt beskyttet kode genereret af IBM Security Trusteer Mobile SDK, og som kan indbygges og integreres i de af Kundens beskyttede, enkeltstående iOS- eller Android-mobilapplikationer, som Kunden abonnerer på IBM SaaS-dækning til ("Kundens integrerede mobilapp").

IBM Security Trusteer Mobile SDK for Retail findes i pakker med 100 Kvalificerede Deltagere eller i pakker med 100 Client-enheder, og IBM Security Trusteer Mobile SDK for Business findes i pakker med 10 Kvalificerede Deltagere eller i pakker med 10 Client-enheder.

Kunden (og et ubegrænset antal medarbejdere med relevant tilladelse) kan modtage begivenhedsdatarapportering og vurdering af risikotendenser. Via Kundens integrerede mobilapp kan Kunden modtage risikoanalyser og oplysninger om mobilenheder, som tilhører Kvalificerede Deltagere, der har downloadet Kundens integrerede mobilapp. Kunden kan derudfra formulere en politik for forebyggelse af svindel og træffe tiltag, der begrænser risikoen for svindel. I forbindelse med dette produkt omfatter "mobilenheder" kun mobiltelefoner og tablets og ikke personlige computere og Mac-computere.

Kunden kan:

a. bruge IBM Security Trusteer Mobile SDK internt alene med henblik på at udvikle Kundens integrerede mobilapp,

b. indbygge den Redistribuérbare komponent (kun i objektkodeformat) som en integreret, ikke-adskillelig del af Kundens integrerede mobilapp. Enhver ændret eller sammenlagt del af den Redistribuérbare komponent er – i henhold til denne licensbevilling – underlagt betingelserne i disse Vilkår for brug, og

c. markedsføre og distribuere den Redistribuérbare komponent med henblik på downloadning på Kvalificerede Deltageres mobile udstyr eller på en Client-enhed. Det er dog en forudsætning, at:

- Medmindre det udtrykkeligt er tilladt i denne Aftale, må Kunden ikke (1) bruge, kopiere, ændre eller distribuere SDK, (2) udføre reverse assembling, reverse compiling eller på anden måde oversætte eller benytte reverse engineering af SDK, medmindre andet gælder ifølge ufravigelig lovbestemmelse, (3) udleje, lease eller give SDK i underlicens, (4) fjerne eventuelle copyrightfiler eller filer med andre angivelser (notice), som findes i den Redistribuérbare komponent, (5) bruge samme stinavn som de oprindelige Redistribuérbare filer/moduler og (6)

bruge IBM's, IBM's licensgiveres eller distributørers navne eller varemærker i forbindelse med markedsføring af Kundens integrerede mobilapp uden forudgående skriftlig tilladelse fra IBM eller licensgiveren eller distributøren.

- Den Redistribuérbare komponent skal fortsat være integreret på en måde, så den ikke kan adskilles fra Kundens integrerede mobilapp. Den Redistribuérbare komponent skal kun være i objektkodeform og skal overholde alle retningslinjer, vejledninger og specifikationer i SDK og den tilhørende dokumentation. Slutbrugerlicensaftalen for Kundens integrerede mobilapp skal indeholde oplysninger til slutbrugeren om, at den Redistribuérbare komponent ikke må i) bruges til andet formål end at aktivere Kundens integrerede mobilapp, ii) kopieres (undtagen med henblik på back-up), iii) videredistribueres eller overføres, iv) demonteres, dekompileres eller på anden måde ændres, medmindre det specifikt er tilladt ifølge ufravigelig lovbestemmelse. Kundens licensaftale skal beskytte IBM i mindst samme grad som vilkårene i denne Aftale.
- SDK må kun implementeres som del af Kundens interne miljø til udvikling og test af enheder på Kundens angivne testmobilenheder. Kunden har ikke tilladelse til at bruge SDK til behandling af produktionsbelastninger, simulering af produktionsbelastninger og test af kodes, applikationers eller systemers skalérbarhed. Kunden har ikke tilladelse til at bruge nogen del af SDK til andre formål.

Kunden er ansvarlig for al teknisk assistance til Kundens integrerede mobilapps og til eventuelle ændringer af de Redistribuérbare komponenter, som Kunden har foretaget, og som er tilladt her.

Kunden bemyndiges til at installere og bruge de Redistribuérbare komponenter og IBM Security Mobile SDK alene for at understøtte Kundens brug af IBM SaaS-produktet.

IBM har testet eksempler på applikationer, som er oprettet ved hjælp af de mobile værktøjer i IBM Security Trusteer Mobile SDK (kaldet Mobile Værktøjer) for at fastslå, om de fungerer korrekt sammen med bestemte versioner af de mobile styresystemsplatforme fra Apple (iOS), Google (Android) og andre (under ét kaldet Mobile OS-platforme). Mobile OS-platforme leveret af tredjepart er dog ikke under IBM's kontrol og kan ændres, uden at IBM får besked om det. Medmindre andet fremgår, garanterer IBM derfor ikke, at applikationer eller anden form for output, som er oprettet ved hjælp af Mobile Værktøjer, fungerer korrekt på, sammen med eller er kompatible med andre Mobile OS-platforme eller mobile enheder.

Kunden skal oprette, opbevare og levere til IBM og IBM's revisorer nøjagtige skriftlige registreringer, output fra systemværktøjer og anden systeminformation, der er tilstrækkelig til at påvise, at Kundens brug af IBM Security Trusteer Mobile SDK er i overensstemmelse med betingelserne i disse Vilkår for brug.

5. Implementering af IBM SaaS Fraud Protection-produkter

Kundens basisabonnement omfatter de nødvendige opsætnings- og indledende implementeringaktiviteter, herunder indledende opstart én gang, konfiguration, Splash-skabelon, test og uddannelse.

Tillægsydelser kan fastlægges i en separat aftale mod betaling af et ekstra gebyr.

Bilag B

IBM tilbyder følgende aftale om Serviceniveau (SLA) for tilgængelighed for IBM SaaS-produktet. Aftalen finder anvendelse, hvis den er angivet i Kundens Transaktionsdokument:

Den version af denne SLA, som gælder på tidspunktet for Kundens abonnements ikrafttrædelse eller fornyelse, er gældende for aftalen. Kunden er indforstået med, at denne SLA ikke udgør en garanti.

1. Definitioner

a. **Autoriseret Kontaktperson** – betyder den person, som Kunden over for IBM har udpeget som autoriseret til at fremsende krav i henhold til denne SLA.

b. **Begivenhed** – betyder en omstændighed eller en række omstændigheder, som samlet betyder, at et Serviceniveau ikke overholdes.

c. **Force Majeure** – betyder naturkatastrofer, terrorisme, faglige aktioner, brand, oversvømmelse, jordskælv, optøjer, krig, offentlig regulering, offentlige påbud eller restriktioner, virus, DOS-angreb (denial of service) og anden ondsindet adfærd, svigt i forbindelser til forsyningsværker og netværk eller enhver anden form for manglende IBM SaaS-tilgængelighed, som ligger uden for IBM's rimelige kontrol.

d. **Kontraheret Måned** – betyder hver hele måned i IBM SaaS-produktets løbetid, målt fra midnat den første dag i måneden til og med kl. 23.59 den sidste dag i måneden.

e. **Krav** – betyder et krav, som den Autoriserede Kontaktperson har sendt til IBM i henhold til vilkårene i denne SLA, og som indeholder en påstand om, at et Serviceniveau ikke er opfyldt i en måned, som er omfattet af aftalen (Kontraheret Måned).

f. **Krediteringsbeløb på grund af manglende tilgængelighed (Availability Credit)** – betyder det beløb, IBM tilbyder i forbindelse med et valideret krav. Availability Credit tilbydes i form af et krediteringsbeløb eller en rabat på en senere faktura for betaling af abonnement på IBM SaaS-produktet.

g. **Kunde** – betyder en enhed, som abonnerer på IBM SaaS-produktet direkte hos IBM, og som ikke har misligholdt en væsentlig forpligtelse, herunder en betalingsforpligtelse, i henhold til Kundens aftale med IBM om IBM SaaS-produktet.

h. **Nedetid** – betyder den tid, hvor produktionssystemets behandling af Serviceydelsen er standset, og hvor alle Kundens brugere ikke kan bruge alle de dele af Servicen, som de har de relevante tilladelser til at bruge. Nedetid omfatter ikke den tid, hvor en Serviceydelse ikke er tilgængelig som følge af:

- Planlagt Systemnedetid.
- Force majeure.
- Problemer med kunde- eller tredjepartsapplikationer, -udstyr eller -data.
- Handlinger eller undladelser fra Kundens eller tredjeparts side, herunder det, at en person får adgang til IBM SaaS-produktet ved brug af Kundens kodeord eller udstyr.
- Manglende overholdelse af de krævede systemkonfigurationer og understøttede platforme, som giver adgang til IBM SaaS-produktet, eller
- IBM's overholdelse af de design, specifikationer eller instruktioner, som Kunden har givet, eller som tredjepart har givet på Kundens vegne.

i. **Planlagt Systemnedetid** – betyder planlagt afbrydelse af IBM SaaS-produktet med vedligeholdelsesformål for øje.

j. **Serviceniveau** – betyder den standard, der er angivet nedenfor, og som IBM bruger som mål for, om IBM leverer det Serviceniveau, IBM skal, i henhold til denne SLA.

2. Availability Credits

a. Før Kunden kan indsende et Krav, skal Kunden have oprettet en problemrapport (ticket) for hver Begivenhed hos den IBM-kundesupporthelpdesk, som tager sig af det relevante IBM SaaS-produkt. Det skal ske i henhold til IBM's procedurer for rapportering af problemer med problemklassificeringskode 1 (Severity 1). Kunden skal give alle nødvendige oplysninger om Begivenheden og i rimeligt omfang hjælpe IBM med fejlfinding og problemløsning i forbindelse med Begivenheden, som det kræves ved en problemrapportering med klassificeringskode 1. Sådanne rapporter skal være registreret inden for 24 timer, efter at Kunden første gang opdagede, at Begivenheden påvirkede Kundens brug af IBM SaaS-produktet.

b. Kundens Autoriserede Kontaktperson skal indsende Kravet om Availability Credit senest tre arbejdsdage efter udgangen af den Kontraherede Måned, som Kravet omfatter.

c. Kundens Autoriserede Kontaktperson skal give IBM alle relevante oplysninger, som vedrører Kravet, herunder f.eks. detaljerede beskrivelser af alle relevante Begivenheder og af det Serviceniveau, som Kunden hævder ikke er opfyldt.

d. IBM måler internt den samlede Nedetid for hver Kontraheret Måned, som gælder for det tilhørende Serviceniveau, der vises i tabellen nedenfor. Availability Credits baseres på varigheden af Nedetiden, målt fra det tidspunkt, som Kunden har rapporteret, at Kunden første gang blev påvirket af Nedetiden. Hvis Kunden rapporterer, at der er indtruffet en Begivenhed med Applikationsnedetid og en Begivenhed med Nedetid mht. Behandling af Indgående Data samtidigt, så behandler IBM de overlappende nedetidsperioder som en enkelt nedetidsperiode, og ikke som to separate nedetidsperioder. IBM anvender den højeste, relevante Availability Credit til hvert gyldigt Krav, baseret på det opnåede Serviceniveau i hver enkelt Kontraheret Måned, som vist i tabellen nedenfor. IBM er ikke ansvarlig for flere Availability Credit-beløb for samme Begivenhed(er) i samme Kontraherede Måned.

e. For så vidt angår pakkede Serviceydelser, det vil sige individuelle IBM SaaS-produkter, der pakkes og sælges sammen til én samlet pris, beregnes Availability Credit på basis af den samlede månedlige pris på de pakkede Serviceydelser og ikke på basis af det månedlige abonnementsgebyr for hvert enkelt IBM SaaS-produkt. Kunden kan kun indsende et Krav vedrørende ét individuelt IBM SaaS-produkt i en pakke i en Kontraheret Måned, og IBM hæfter ikke for Availability Credits for mere end ét IBM SaaS-produkt i en pakke i en Kontraheret Måned.

f. Hvis Kunden har købt IBM SaaS-produktet fra en godkendt IBM-forhandler i en videresalgstransaktion, hvor IBM har det primære ansvar for at opfylde forpligtelserne i forbindelse med IBM SaaS-produktet og aftalen om Serviceniveau (SLA), baseres Availability Credit på den dengang gældende RSVP-pris (Relationship Suggested Value Price) for IBM SaaS-produktet for den Kontraherede Måned, som kravet omfatter, nedsat med 50 %.

g. Den samlede Availability Credit, som Kunden får tildelt for en Kontraheret Måned, kan under ingen omstændigheder overstige 10 % af en tolvtedel (1/12) af det beløb, Kunden betaler IBM årligt for IBM SaaS-produktet.

h. IBM foretager et rimeligt skøn ved validering af Krav, baseret på de oplysninger, der er tilgængelige i IBM's registreringer, og disse registreringer har forrang i tilfælde af en uoverensstemmelse med data i Kundens egne registreringer.

i. De Availability Credits, som Kunden får tilbudt i henhold til denne SLA, er Kundens eneste retsmiddel i forbindelse med et Krav.

3. Serviceniveauer

IBM SaaS-tilgængelighed i en Kontraheret Måned

Opnået Serviceniveau (i en Kontraheret Måned)	**Availability Credit (% af den månedlige abonnementsbetaling for den Kontraherede Måned, som er genstand for Kravet)**
< 99,5 %	2 %
< 98,0 %	5 %
< 96,0 %	10 %

"Opnået Serviceniveau", udtrykt i procent, beregnes på denne måde: (a) det samlede antal minutter i en Kontraheret Måned minus (b) nedetid i alt i minutter i en Kontraheret Måned divideret med (c) det samlede antal minutter i en Kontraheret Måned.

Eksempel: 250 minutters Nedetid i alt i en Kontraheret Måned

43.200 minutter i alt i en Kontraheret Måned på 30 dage - 250 minutters Nedetid = 42.950 minutter _____ 43.200 minutter i alt	= 2 % Availability Credit for et Opnået Serviceniveau på 99,4 % i den Kontraherede Måned

3.1 Undtagelser

Denne SLA gælder kun IBM-kunder. Denne SLA gælder ikke følgende:

- Beta- og prøveservices.
- Ikke-produktionsmiljøer, herunder for eksempel test, retablering efter katastrofe, kvalitetssikring eller udvikling.
- Krav fremsat af en IBM-Kundes brugere, gæster, deltagere og tilladte inviterede, som bruger IBM SaaS-produktet.
- Hvis Kunden har misligholdt en væsentlig forpligtelse i henhold til Vilkår for brug, herunder f.eks. misligholdelse af betalingsforpligtelser.