# IBM Security Trusteer Fraud Protection

Bruksbetingelsene ("Bruksbetingelsene" eller "ToU") består av denne IBM Bruksbetingelser – Betingelser for et bestemt IBM SaaS-tilbud ("Betingelser for et bestemt IBM SaaS-tilbud") og dokumentet med tittelen IBM Bruksbetingelser – Generelle betingelser ("Generelle betingelser") som er tilgjengelig på følgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Hvis det oppstår motstrid, gjelder Betingelser for et bestemt IBM SaaS-tilbud foran Generelle betingelser. Kunden aksepterer disse Bruksbetingelsene ved å bestille, åpne eller bruke IBM SaaS.

Bruksbetingelsene er underlagt IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement eller IBM International Agreement for Selected IBM SaaS Offerings, avhengig av hva som er aktuelt, ("Avtalen"), som sammen med Bruksbetingelsene utgjør den fullstendige avtalen.

## 1. IBM SaaS

Følgende IBM SaaS-løsninger er dekket av disse Betingelsene for et bestemt IBM SaaS-tilbud:

### 1.1 IBM SaaS Rapport-løsninger

- 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-løsninger

- 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 IBM SaaS Mobile-løsninger

- 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. Målenheter for omkostninger

IBM SaaS selges under en av følgende målenhet(er) for omkostninger som spesifisert i Transaksjonsdokumentet:

a. **Kvalifisert deltaker** (Eligible Participant) er en målenhet for anskaffelse av IBM SaaS. Hver person eller enhet som er kvalifisert for å delta i et tjenesteleveringsprogram som administreres eller spores av IBM SaaS, er en Kvalifisert deltaker. Det må anskaffes tilstrekkelig antall rettigheter for å dekke alle Kvalifiserte deltakere som administreres eller spores i IBM SaaS i løpet av måleperioden som er oppgitt i Kundens Transaksjonsdokument.

   Hvert tjenesteleveringsprogram som administreres av IBM SaaS, analyseres separat, og resultatene adderes. Personer eller enheter som er kvalifisert for flere tjenesteleveringsprogrammer, krever separate rettigheter.

   For disse løsningene omfatter et tjenesteleveringsprogram en enkelt Business- eller Retail-applikasjon hos Kunden med en hovedside for pålogging og tilknyttede sider for hver Business- eller Retail-applikasjon. En Kvalifisert deltaker (Eligible Participant) er en sluttbruker hos Kunden som har påloggingslegitimasjon for Business- eller Retail-applikasjonen.

b. **Klientenhet** (Client Device) er en målenhet for anskaffelse av IBM SaaS. En Klientenhet er en enkelt brukers databehandlingsenhet eller sensor- eller telemetrienhet med spesiell funksjon, som ber om utføring av eller mottar for utføring et sett med kommandoer, prosedyrer eller applikasjoner fra, eller leverer data til, et annet databehandlingssystem som vanligvis kalles en server, eller på annen måte er styrt av serveren. Flere Klientenheter kan dele tilgangen til en felles server. En Klientenhet kan ha noen behandlingsmuligheter eller være programmerbar slik at brukeren kan utføre arbeid. Kunden må anskaffe rettigheter for hver Klientenhet som kjører, leverer data til, bruker tjenester levert av eller på annen måte får tilgang til IBM SaaS i måleperioden som er oppgitt i Kundens Transaksjonsdokument.

## 3. Priser og fakturering

Beløpet som skal betales for IBM SaaS, er oppgitt i et Transaksjonsdokument.

### 3.1 Pris for del av måned

Prisen for en del av en måned som fremkommer i Transaksjonsdokumentet, kan være en forholdsmessig beregnet pris.

## 4. Overholdelse og revisjon

Tilgang til IBM Security Trusteer Fraud Protection-løsningene er begrenset til et maksimalt antall Kvalifiserte deltakere eller Klientenheter angitt i Transaksjonsdokumentet. Kunden skal sørge for at antallet Kvalifiserte deltakere eller Klientenheter ikke overstiger det maksimale antallet som er angitt i Transaksjonsdokumentet.

Det kan utføres revisjon for å kontrollere at kravet til maksimalt antall Kvalifiserte deltakere eller Klientenheter er overholdt.

## 5. Alternativer for fornyelse av Abonnementsperiode for IBM SaaS

Det fremkommer i Kundens Transaksjonsdokument om IBM SaaS blir fornyet ved slutten av Abonnementsperioden, ved en av følgende beskrivelser:

### 5.1 Automatisk fornyelse

Hvis Kundens Transaksjonsdokument angir at Kundens fornyelse er automatisk, kan Kunden si opp IBM SaaS-abonnementsperioden som er i ferd med å utløpe, med skriftlig forhåndsvarsel til Kundens IBM-salgsrepresentant eller IBM Business Partner minst 90 dager før utløpsdatoen som er angitt i Transaksjonsdokumentet. Hvis IBM eller Kundens IBM Business Partner ikke mottar et slikt oppsigelsesvarsel innen utløpsdatoen, blir den utløpende Abonnementsperioden fornyet automatisk enten for ett år eller for samme varighet som den opprinnelige Abonnementsperioden, avhengig av hva som fremgår av Transaksjonsdokumentet.

### 5.2 Fortløpende fakturering

Når Transaksjonsdokumentet angir at Kundens fornyelse er fortløpende, har Kunden fortsatt tilgang til IBM SaaS og blir fortløpende fakturert for bruken av IBM SaaS. Hvis Kunden ønsker å opphøre med bruken av IBM SaaS og stoppe den fortløpende faktureringsprosessen, må Kunden gi IBM eller Kundens IBM Business Partner 90 dagers skriftlig forhåndsvarsel om oppsigelse av IBM SaaS. Ved oppsigelse av Kundens tilgang blir Kunden fakturert for alle utestående beløp for tilgang i måneden oppsigelsen trer i kraft.

### 5.3 Fornyelse nødvendig

Når Transaksjonsdokumentet angir at Kundens fornyelsestype er "terminate", avsluttes IBM SaaS ved utløpet av Abonnementsperioden, og Kundens tilgang til IBM SaaS blir fjernet. Hvis Kunden ønsker fortsatt bruk av IBM SaaS etter sluttdatoen, må Kunden sende en bestilling til Kundens IBM-salgsrepresentant eller IBM Business Partner for å anskaffe en ny Abonnementsperiode.

## 6. Teknisk støtte

Teknisk støtte for IBM SaaS er tilgjengelig for Kunden og Kundens Kvalifiserte deltakere til hjelp ved deres bruk av IBM SaaS.

Standardstøtte (Standard Support) er inkludert i abonnementet for alle løsninger. Trusteer Rapport Mandatory Service, som er en tilleggstjeneste for Trusteer Rapport, har som forutsetning et Premium Support-abonnement for Trusteer Rapport-basisabonnementet.

For hver IBM SaaS-løsning er et Premium Support-abonnement tilgjengelig mot betaling, unntatt for IBM Security Trusteer Mobile SDK-løsningene og IBM Security Trusteer Rapport Mandatory Service-løsningene.

**Standardstøtte:**

- Støtte 8.00 - 17.00 lokal tid.
- Kunden og Kundens Kvalifiserte deltakere kan sende inn problemrapporter elektronisk, slik det er beskrevet i Software as a Service [SaaS] Support Handbook.
- Kunden har tilgang til portalen for kundestøtte for varsler, dokumenter, saksrapporter og spørsmål og svar, på: http://www-01.ibm.com/software/security/trusteer/support/.
- Informasjon om alternativer for støtte og nærmere detaljer finnes i IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

**Premium-støtte:**

- Støtte 24x7 (hele døgnet, alle ukens dager) for alle alvorsgrader.
- Kunden kan kontakte støttepersonell direkte via telefon.
- Kunden og Kundens Kvalifiserte deltakere kan sende inn problemrapporter elektronisk, slik det er beskrevet i Software as a Service [SaaS] Support Handbook.
- Kunden har tilgang til portalen for kundestøtte for varsler, dokumenter, saksrapporter og spørsmål og svar, på: http://www-01.ibm.com/software/security/trusteer/support/.
- Informasjon om alternativer for støtte og nærmere detaljer finnes i IBM Software as a Service [SaaS] Support Handbook: http://www-01.ibm.com/software/support/handbook.html.

# 7. Tilleggsbetingelser for IBM SaaS

## 7.1 Safe Harbor-overholdelse

IBM overholder U.S. – EU Safe Harbor Framework utarbeidet av U.S. Department of Commerce i samarbeid med Europakommisjonen. IBM Security Trusteer-produktene er inkludert i IBMs EU-U.S. Safe Harbor-sertifisering. Det finnes mer informasjon om Safe Harbor og en liste over Safe Harbor-selskaper her: http://export.gov/safeharbor/.

## 7.2 Økning i Kundens årlige abonnementspris

IBM forbeholder seg rett til å justere abonnementsprisen for IBM SaaS høyst en gang per år (12 måneder) med en prosentsats bestemt av IBM som ikke skal overstige 3 %. Justeringen av abonnementsprisen skal tre i kraft på årsdagen for startdatoen for den første dekningsperioden. Denne prisjusteringen endrer ikke Kundens rettigheter til IBM SaaS eller målenheten for omkostninger som IBM SaaS er anskaffet under. IBM Business Partnere er selvstendige og fastsetter alene sine priser og betingelser uavhengig av IBM.

## 7.3 Premium-støtte

Kunden har rett til Premium-støtte kun for IBM SaaS-løsninger der Kunden har abonnert på den tilknyttede Premium Support-løsningen.

## 7.4 Lovlig bruk og samtykke

**Tillatelse til å samle inn og behandle data**

IBM SaaS er utformet for å hjelpe Kunden med å forbedre Kundens sikkerhetsmiljø og data. IBM SaaS samler inn informasjon fra Kvalifiserte deltakere og Klientenheter som virker sammen med Business- eller Retail-applikasjonene som Kunden har abonnert på IBM SaaS-dekning for. IBM SaaS samler inn informasjon som alene eller i kombinasjon kan anses som Personopplysninger i enkelte jurisdiksjoner. Personopplysninger er enhver informasjon som kan brukes til å identifisere en bestemt person, for eksempel et navn, en e-postadresse, en privatadresse, eller et telefonnummer som er levert til IBM for lagring, behandling eller overføring på vegne av Kunden.

Fremgangsmåtene for innsamling og behandling av data kan oppdateres for å forbedre funksjonaliteten i IBM SaaS. Et dokument med en fullstendig beskrivelse av fremgangsmåtene for innsamling og behandling oppdateres ved behov og vil på forespørsel være tilgjengelig for Kunden. Kunden gir IBM tillatelse til å samle inn denne informasjonen og behandle den i overensstemmelse med punktene Overføring over landegrenser og Beskyttelse av personopplysninger i disse Bruksbetingelsene, og punktet Beskyttelse av personopplysninger og datasikkerhet i IBM Bruksbetingelser – Generelle betingelser.

**For IBM Security Trusteer Pinpoint-løsninger:**

Innsamlede data kan omfatte brukerens IP-adresse, kryptert eller enveis hash-verdi for bruker-ID, domeneinformasjonskapsler hvis de ikke er filtrert ut, besøk i beskyttede Applikasjoner eller på nettsteder for nettfisking (phishing), geografisk plassering og legitimasjon oppgitt på nettfiskingsnettsteder.

**For IBM Security Trusteer Mobile SDK- og IBM Security Trusteer Mobile Browser-løsninger:**

Innsamlede data kan omfatte brukerens IP-adresse, kryptert eller enveis hash-verdi for bruker-ID, geografisk plassering, besøk i beskyttede Applikasjoner, SIM-kortinformasjon, enhetsnavn og tilknytning til Kunden.

**For IBM Security Trusteer Rapport-løsninger:**

Innsamlede data kan omfatte brukerens IP-adresse, kryptert eller enveis hash-verdi for bruker-ID, sikkerhetshendelser, brukernavn og e-postadresse gitt i den hensikt å kunne kontakte IBM for å be om kundestøtte, tilknytning til Kunden, kryptert passord oppgitt på beskyttede nettsteder, besøk i beskyttede Applikasjoner og på nettfiskingsnettsteder, kryptert betalingskortnummer samt filer og data samlet inn eksternt av IBMs personell for å undersøke mistenkt skadelig programvare, skadelige aktiviteter eller funksjonsfeil.

**Samtykke fra den registrerte:**

Bruk av IBM SaaS kan implisere flere lover eller forskrifter. IBM SaaS kan kun brukes for lovlige formål og på lovlig måte. Kunden aksepterer å bruke IBM SaaS i overensstemmelse med, og påtar seg alt ansvar for å rette seg etter, gjeldende lovgivning og bestemmelser.

**For IBM Security Trusteer Pinpoint- og IBM Security Trusteer Mobile SDK-løsninger:**

Kunden bekrefter at Kunden har innhentet eller skal innhentet fullt informert samtykke, tillatelser eller lisenser som er nødvendige for lovlig bruk av IBM SaaS og for IBMs innsamling og behandling av informasjonen gjennom IBM SaaS.

**For IBM Security Trusteer Rapport- og IBM Security Trusteer Mobile Browser-løsninger:**

Kunden autoriserer IBM for å innhente fullt informert samtykke som er nødvendig for lovlig bruk av IBM SaaS og for innsamling og behandling av informasjonen slik det er beskrevet i lisensavtalen for sluttbrukere på https://www.trusteer.com/support/end-user-license-agreement. Dersom Kunden bestemmer at Kunden (og ikke IBM) skal håndtere kommunikasjonen med sluttbrukerne vedrørende deres samtykke, bekrefter Kunden at Kunden har innhentet eller skal innhentet fullt informert samtykke, tillatelser eller lisenser som er nødvendige for lovlig bruk av IBM SaaS og for IBMs innsamling og behandling av informasjonen som Kundens databehandler gjennom IBM SaaS.

## 7.5 Overføring over landegrenser

Kunden aksepterer at IBM kan behandle innhold, inkludert Personopplysninger, i henhold til aktuelle lover og krav, over en landegrense til behandlere og underbehandlere i følgende land utenfor EØS-området og land som Europakommisjonen anser å ha et tilstrekkelig vernenivå: USA.

## 7.6 Beskyttelse av personopplysninger

Hvis Kunden gjør Personopplysninger tilgjengelig for IBM SaaS i EU-medlemsstater, Island, Liechtenstein, Norge eller Sveits, eller hvis Kunden har Kvalifiserte deltakere eller Klientenheter i disse landene, utpeker Kunden som eneste behandlingsansvarlige IBM som databehandler for behandling (slik disse betegnelsene er definert i EU-direktiv 95/46/EF) av Personopplysninger. IBM skal bare behandle slike Personopplysninger i den utstrekning det er nødvendig for å gjøre IBM SaaS-løsningen tilgjengelig i henhold til IBMs publiserte beskrivelser av IBM SaaS, og Kunden bekrefter at slik behandling er i overensstemmelse med Kundens instruksjoner. IBM skal varsle Kunden i rimelig tid på forhånd hvis IBM gjør en endring med vesentlig betydning av behandlingssted og måten IBM sikrer Personopplysninger på som en del av IBM SaaS. Kunden kan avbryte gjeldende Abonnementsperiode for aktuell IBM SaaS med skriftlig varsel til IBM innen tretti (30) dager etter IBMs varsel om endringen til Kunden. Kunden aksepterer at IBM kan behandle innhold, inkludert Personopplysninger, over en landegrense til følgende behandlere og underbehandlere:

| Navn på behandler/underbehandler | Rolle (databehandler eller underbehandler) | Sted* |
|---|---|---|
| IBMs avtaleenhet | Behandler | Som angitt i Transaksjonsdokumentet |
| Amazon Web Services LLC | Underbehandler | 410 Terry Ave. N<br>Seattle, WA 98109<br>USA |
| Connectria Corp. | Underbehandler | 10845 Olive Blvd., Suite 300<br>St. Louis, MO 63141<br>USA |
| IBM Israel Ltd. | Underbehandler | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |

| Navn på behandler/underbehandler | Rolle (databehandler eller underbehandler) | Sted* |
|---|---|---|
| IBM Corp | Underbehandler | 1 New Orchard Rd.<br>Armonk, NY 10504<br>USA |

Kunden aksepterer at IBM med skriftlig varsel kan endre denne listen over land når IBM med rimelighet anser det som nødvendig for å kunne levere IBM SaaS.

Kunden aksepterer at for tjenester som leveres gjennom det tyske datasenteret, bestemt under leveringsprosessen, kan IBM behandle innhold, inkludert Personopplysninger, over en landegrense til følgende behandlere og underbehandlere:

| Navn på behandler/underbehandler | Rolle (databehandler eller underbehandler) | Sted* |
|---|---|---|
| IBMs avtaleenhet | Behandler | Som angitt i Transaksjonsdokumentet |
| Amazon Web Services (Germany) | Underbehandler | München, Tyskland |
| IBM Israel Ltd. | Underbehandler | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |

Kunden aksepterer at for tjenester som leveres gjennom det japanske datasenteret, bestemt under leveringsprosessen, kan IBM behandle innhold, inkludert Personopplysninger, over en landegrense til følgende behandlere og underbehandlere:

| Navn på behandler/underbehandler | Rolle (databehandler eller underbehandler) | Sted* |
|---|---|---|
| IBMs avtaleenhet | Behandler | Som angitt i Transaksjonsdokumentet |
| Amazon Web Services (Japan) | Underbehandler | Tokyo, Japan |
| IBM Israel Ltd. | Underbehandler | 94 Derech Em-Hamoshavot<br>49527 Petach-Tikva<br>Israel |

* Stedene som er angitt i tabellene ovenfor, inneholder adressene til behandlernes eller underbehandlernes hovedkontorer. Datasentrene befinner seg i samme land.

Partene eller deres aktuelle tilknyttede selskaper kan inngå separate avtaler ved bruk av EUs uendrede standardkontrakt i deres aktuelle roller, i henhold til Beslutning 2010/87/EU, med valgfrie klausuler fjernet. Alle konflikter eller forpliktelser som oppstår i forbindelse med disse avtalene, selv om de er inngått av tilknyttede selskaper, skal behandles av partene som om konflikten eller forpliktelsen oppstod mellom disse partene under betingelsene i denne Avtalen.

# Vedlegg A

## 1. IBM SaaS-løsninger

IBM tilbyr disse tjenestene som frittstående tjenester og løsninger, eller som tilleggstjenester og tilleggsløsninger. IBM SaaS-løsningene som er bestilt, fremkommer i Kundens kjøpsbevis (PoE).

### 1.1 Definisjon av Business- og Retail-applikasjoner

IBM Security Trusteer Fraud-produktene lisensieres for bruk sammen med bestemte typer av Applikasjoner. En Applikasjon er definert som en av følgende typer: Retail eller Business. Egne løsninger er tilgjengelige for Retail-applikasjoner og Business-applikasjoner.

- En Retail-applikasjon er definert som en online bankapplikasjon, mobilapplikasjon eller applikasjon for e-handel, som er utformet til bruk for forbrukere. Kundens retningslinjer kan klassifisere enkelte mindre virksomheter som kvalifisert for tilgang til Retail-applikasjoner.
- En Business-applikasjon er definert som en online bankapplikasjon, mobilapplikasjon eller applikasjon for e-handel, som er utformet til bruk for bedrifter, institusjoner eller liknende enheter, eller en applikasjon som ikke tilhører kategorien Retail.

### 1.2 Basisabonnementer for IBM SaaS-løsninger

**Business-løsninger:**

- 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-løsninger:**

- 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

For hver Business- og Retail-løsning finnes det et tilknyttet Premium Support-produkt som er tilgjengelig mot betaling, unntatt for IBM Security Trusteer Mobile SDK-løsningene.

### 1.3 IBM SaaS-tilleggsabonnementer for IBM Security Trusteer Rapport-løsningene

Tilleggsløsninger som er tilgjengelige for 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

Tilleggsløsninger som er tilgjengelige for 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

For hver Business- og Retail-tilleggstjeneste for IBM Security Trusteer Rapport-løsningene, unntatt for IBM Security Trusteer Rapport Mandatory Service-tilleggstjenestene, finnes det et tilknyttet Premium Support-produkt som er tilgjengelig mot betaling.

Abonnement på IBM Security Trusteer Rapport for Business eller IBM Security Trusteer Rapport for Retail er en forutsetning for de tilknyttede IBM SaaS-tilleggsabonnementene angitt i dette punktet.

### 1.4 IBM SaaS-tilleggsabonnementer for IBM Security Trusteer Pinpoint Malware Detection-løsningene

Tilleggsløsninger som er tilgjengelige for 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

Tilleggsløsninger som er tilgjengelige for 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

Premium Support-abonnement er tilgjengelig mot betaling for hver av IBM SaaS-tilleggsløsningene som er angitt i dette punktet.

Abonnement på IBM Security Trusteer Pinpoint Malware Detection for Business-løsninger eller IBM Security Trusteer Pinpoint Malware Detection for Retail-løsninger er en forutsetning for de tilknyttede IBM SaaS-tilleggsabonnementene angitt i dette punktet.

### 1.5 Andre IBM SaaS-tilleggsabonnementer

Eventuelle IBM SaaS-tilleggsabonnementer for basisabonnementene ovenfor som ikke er angitt her, tilgjengelige nå eller under utvikling, anses ikke som en oppdatering og må tildeles separat.

### 1.6 Definisjoner

**Kontoinnehaver** er Kundens sluttbruker som har installert klientaktiveringsprogramvaren, akseptert lisensavtalen for sluttbrukere ("EULA" (End User License Agreement)) og vært autentisert minst en gang for Kundens Retail- eller Business-applikasjon som Kunden har abonnert på IBM SaaS-dekning for.

**Klientprogramvare for kontoinnehavere** er IBM Security Trusteer Rapport-klientaktiveringsprogramvaren eller IBM Security Trusteer Mobile Browser-klientaktiveringsprogramvaren eller en annen klientaktiveringsprogramvare som leveres sammen med enkelte IBM SaaS-abonnementer for å installeres på sluttbrukernes enhet.

**Trusteer-oppstartsbilde** er oppstartsbildet som leveres Kunden basert på tilgjengelige oppstartsbildemaler.

**Landingsside** er den IBM-vertede siden som leveres Kunden sammen med Kundens oppstartsbilde og nedlastbare Klientprogramvare for kontoinnehavere.

## 2. IBM Security Trusteer Rapport-løsninger

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

Trusteer Rapport gir et lag med beskyttelse mot nettfiskings- og MitB-angrep (Man-in-the-Browser) fra skadelig programvare. Ved hjelp av et verdensomfattende nettverk med flere titalls millioner sluttpunkter samler IBM Security Trusteer Rapport inn informasjon om aktive nettfiskingsangrep og angrep av skadelig programvare mot organisasjoner over hele verden. IBM Security Trusteer Rapport benytter atferdsalgoritmer som skal blokkere nettfiskingsangrep og forhindre installering og kjøring av skadelig programvare av typen MitB.

Denne IBM SaaS-løsningen benytter måleverdien Kvalifisert deltaker. Business-løsningen selges i pakker på 10 Kvalifiserte deltakere. Retail-løsningen selges i pakker på 100 Kvalifiserte deltakere.

Denne IBM SaaS-løsningen omfatter følgende:

a. Trusteer Management Application ("TMA"):

   TMA er tilgjengelig i det nettskyvertede IBM Security Trusteer-miljøet, og gjennom denne applikasjonen kan Kunden (og et ubegrenset antall av Kundens autoriserte personell) (i) motta hendelsesdatarapporter og risikovurderinger, (ii) vise, konfigurere og definere policyer knyttet til

rapportering av hendelsesdata, og (iii) vise konfigurasjonen av klientaktiveringsprogramvaren som er allment lisensiert under en lisensavtale for sluttbrukere ("EULA") vederlagsfritt tilgjengelig for nedlasting til en Kvalifisert deltakers datamaskin eller enhet (PC/MAC), også kjent som Trusteer Rapport Software Suite ("Klientprogramvare for kontoinnehavere"). Kunden kan bare markedsføre Klientprogramvaren for kontoinnehavere ved bruk av Trusteer-oppstartsbildet eller Rapport-APIen, og Kunden kan ikke bruke Klientprogramvaren for kontoinnehavere til Kundens interne forretningsoperasjoner eller til bruk for Kundens ansatte (annet enn ansattes personlige bruk).

b. Webskript:

For tilgang til et nettsted i den hensikt å få tilgang til eller bruke IBM SaaS-løsningene.

c. Hendelsesdata:

Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta hendelsesdata generert fra Klientprogramvare for kontoinnehavere som et resultat av Kontoinnehavernes online-interaksjoner med Kundens Business- eller Retail-applikasjon som Kunden har abonnert på IBM SaaS-dekning for. Hendelsesdata mottas fra Kvalifiserte deltakeres Klientprogramvare for kontoinnehavere som kjører på deres enheter, der den Kvalifiserte deltakeren må ha akseptert EULA samt være autentisert minst en gang for Kundens Business- eller Retail-applikasjon(er), og Kundens konfigurasjon må omfatte innsamling av Bruker-IDer.

d. Trusteer-oppstartsbilde:

Markedsføringsplattformen for Trusteer-oppstartsbildet identifiserer og markedsfører Klientprogramvaren for kontoinnehavere for de Kvalifiserte deltakerne som får tilgang til Kundens Business- og/eller Retail-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for. Kunden kan velge blant tilgjengelige oppstartsbildemaler. Et tilpasset oppstartsbilde kan avtales under en separat avtale eller tjenestebeskrivelse.

Kunden kan akseptere å fremskaffe sine varemerker, logoer eller ikoner til bruk i forbindelse med TMA og kun til bruk sammen med Trusteer-oppstartsbildet og for visning i Klientprogramvaren for kontoinnehavere eller på landingssider som vertes av IBM, og på IBM Security Trusteer-nettstedet. Enhver bruk av Kundens avleverte varemerker, logoer eller ikoner vil være i overensstemmelse med IBMs rimelige retningslinjer vedrørende reklame og bruk av varemerker.

Kunden må abonnere på SaaS-løsningen IBM Security Trusteer Rapport Mandatory Service hvis Kunden ønsker å benytte en type av obligatorisk installering av Klientprogramvaren for kontoinnehavere.

Obligatorisk installering av Klientprogramvaren for kontoinnehavere omfatter, men er ikke begrenset til, enhver type av obligatorisk installering ved hjelp av en mekanisme eller metode som direkte eller indirekte tvinger en Kvalifisert deltaker til å laste ned Klientprogramvaren for kontoinnehavere, eller en metode, verktøy, prosedyre, avtale eller mekanisme som ikke er opprettet eller godkjent av IBM, opprettet for å omgå lisensieringskravene for denne obligatoriske installeringen av Klientprogramvaren for kontoinnehavere.

## 2.2 Valgfrie IBM SaaS-tilleggsløsninger for IBM Security Trusteer Rapport for Business og/eller IBM Security Trusteer Rapport for Retail

Abonnement på IBM Security Trusteer Rapport-løsninger er en forutsetning for abonnement på følgende IBM SaaS-tilleggsløsninger. Hvis IBM SaaS er betegnet som "for Business", må en anskaffet IBM SaaS-løsning også være betegnet som "for Business". Hvis IBM SaaS er betegnet som "for Retail", må en anskaffet IBM SaaS-løsning også være betegnet som "for Retail". Kunden mottar hendelsesdata fra Kvalifiserte deltakere som kjører Klientprogramvaren for kontoinnehavere, der den Kvalifiserte deltakeren må ha akseptert EULA samt være autentisert minst en gang for Kundens Business- og/eller Retail-applikasjon(er), og Kundens konfigurasjon må omfatte innsamling av Bruker-IDer.

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

Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta hendelsesdata knyttet til infeksjoner med skadelig programvare og annen sluttpunktsårbarhet på en bestemt Kontoinnehavers datamaskin.

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

Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta varsler om hendelsesdata knyttet til sending av en Kontoinnehavers påloggingslegitimasjon til et mistenkt nettfiskingsnettsted eller mulig bedragersk nettsted. Lovlige online-applikasjoner (URLer) kan ved en feil flagges som nettfiskingsnettsteder, og IBM SaaS kan varsle Kontoinnehavere om at et lovlig nettsted er et nettfiskingsnettsted. I slike tilfeller må Kunden varsle IBM om feilen, og IBM vil rette feilen. Dette er Kundens eneste beføyelse i forbindelse med en slik feil.

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

Kunden kan bruke en forekomst av markedsføringsplattformen for Trusteer-oppstartsbildet til å gi rett til nedlasting av Klientprogramvaren for kontoinnehavere til Kvalifiserte deltakere som får tilgang til Kundens Business- og/eller Retail-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for.

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

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

Kunden kan implementere tilleggsfunksjonalitet fra IBM Security Trusteer Rapport Mandatory Service kun hvis den bestilles og konfigureres for bruk sammen med Kundens Retail- eller Business-applikasjon som Kunden har abonnert på IBM SaaS-dekning for.

## 3. IBM Security Trusteer Pinpoint-løsninger

IBM Security Trusteer Pinpoint er en nettskybasert tjeneste som er utformet for å gi et ekstra lag med beskyttelse, og har som formål å oppdage og utføre utbedring ved nettfiskingsangrep og forsøk på kontoovertakelse. Trusteer Pinpoint kan integreres i Kundens Business- og/eller Retail-applikasjoner der Kunden har abonnert på IBM SaaS-dekning og prosesser for å forhindre svindel.

Denne IBM SaaS-løsningen omfatter følgende:

a. TMA:

   TMA er tilgjengelig i det nettskyvertede IBM Security Trusteer-miljøet, og gjennom denne applikasjonen kan Kunden (og et ubegrenset antall av Kundens autoriserte personell) (i) motta hendelsesdatarapporter og risikovurderinger, og (ii) vise, konfigurere og definere sikkerhetspolicyer samt policyer knyttet til rapportering av hendelsesdata.

b. Webskript og/eller APIer:

   For installering på et nettsted i den hensikt å få tilgang til eller bruke IBM SaaS-løsningene.

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

Ved oppdagelse av skadelig programvare i IBM Security Trusteer Pinpoint Malware Detection-løsninger eller av forsøk på kontoovertakelse i IBM Security Trusteer Pinpoint Criminal Detection-løsninger, må Kunden etterfølge Pinpoint Best Practices Guide. Ikke bruk IBM Security Trusteer Pinpoint Malware Detection-løsninger eller IBM Security Trusteer Pinpoint Criminal Detection-løsninger på noen måte som kan påvirke en Kvalifisert deltakers opplevelse rett etter en oppdagelse av skadelig programvare eller forsøk på kontoovertakelse, slik at det kan bli mulig for andre å linke Kundens handlinger til bruk av IBM Security Trusteer Pinpoint-løsninger (som varsler, meldinger, blokkering av enheter eller blokkering av tilgangen til Business- og/eller Retail-applikasjonen rett etter en oppdagelse av skadelig programvare eller forsøk på kontoovertakelse).

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

Klientløs oppdagelse av mistenkelige aktiviteter for kontoovertakelse i nettlesere som tilkobles en Business- eller Retail-applikasjon, ved hjelp av enhets-ID, oppdagelse av nettfisking og oppdagelse av legitimasjonstyveri gjennom skadelig programvare. IBM Security Trusteer Pinpoint Criminal Detection-løsningene gir et ekstra lag med beskyttelse og har som formål å oppdage forsøk på kontoovertakelse samt levere resultater av risikovurderinger for nettlesere eller mobilenheter (gjennom standard nettleser eller Kundens mobilapplikasjon) som har tilgang til en Business- eller Retail-applikasjon, direkte til Kunden.

a. Hendelsesdata:

Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta hendelsesdata generert som et resultat av Kvalifiserte deltakeres online-interaksjoner med Kundens Business- og/eller Retail-applikasjon(er) som Kunden har abonnert på IBM SaaS-dekning for, eller Kunden kan motta hendelsesdataene levert via et brukergrensesnitt i et bakgrunnsprogram.

### 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-løsningene (PPCD Mobile) er utformet for å gi et ekstra lag med beskyttelse og har som formål å beskytte mot kontoovertakelse og uredelige aktiviteter, ved å identifisere forbrytersk kontotilgang og gi Kunden en anbefaling. Denne IBM SaaS-løsningen samler inn informasjon som kommer fra både Kundens Business- og/eller Retail-applikasjon ved bruk av PPCD Mobile-APIen, og fra Kvalifiserte deltakeres mobilenheter. IBM Security Trusteer PPCD Mobile-løsningene er utformet for å korrelere kompleks informasjon knyttet til Kvalifiserte deltakeres mobilenheter med data fra andre datakilder, som informasjon i sanntid om infeksjon med skadelig programvare og nettfiskingshendelser som er integrert via andre IBM SaaS-løsninger for IBM Security Trusteer beskrevet i disse Bruksbetingelsene.

Kunden kan få tilgang til og bruke IBM Security Trusteer PPCD Mobile-løsningene i det nettskyvertede IBM Security Trusteer-miljøet og motta risikovurderingsdata fra Kvalifiserte deltakeres mobilenheter, som er generert som et resultat av disse mobilenhetenes online-interaksjoner med Kundens Business- eller Retail-applikasjon som Kunden har abonnert på IBM SaaS-dekning for. For disse løsningene omfatter "mobilenheter" bare støttede mobiltelefoner og nettbrett, ikke PC- eller MAC-enheter.

### 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 oppdagelse av nettlesere infisert med skadelig programvare av typen MitB (Man in the Browser), som kobles til en Business- og/eller Retail-applikasjon. IBM Security Trusteer Pinpoint Malware Detection-løsningene gir et ekstra lag med beskyttelse og har som formål å gjøre det mulig for organisasjoner å fokusere på prosesser for å forhindre svindel basert på risiko for skadelig programvare, ved å gi Kunden vurderinger og varsler ved oppdagelse av skadelig programvare av typen MitB.

a. Hendelsesdata:

Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta hendelsesdata generert som et resultat av Kvalifiserte deltakeres online-interaksjoner med Kundens Business- og/eller Retail-applikasjon(er).

b. Advanced Edition:

Advanced Edition for Business og/eller for Retail gir et ekstra lag for oppdagelse og beskyttelse som justeres og tilpasses til Kundens Business- og/eller Retail-applikasjons struktur og flyt, og kan tilpasses til Kundens trusselbilde. Advanced Edition kan innlemmes på forskjellige steder innenfor Kundens Business- og/eller Retail-applikasjoner.

Advanced Edition tilbys Kunden for et minimumsantall på minst 100 000 Kvalifiserte deltakere for Retail eller 10 000 Kvalifiserte deltakere for Business, som tilsvarer 1000 pakker med 100 Kvalifiserte deltakere for Retail eller 1000 pakker med 10 Kvalifiserte deltakere for Business.

c. Standard Edition:

Standard Edition for Business eller for Retail er en løsning som er lett å implementere, og som inneholder kjernefunksjonene i denne IBM SaaS-løsningen, beskrevet her.

## 3.2 Valgfrie IBM SaaS-tilleggsløsninger for 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

For IBM Security Trusteer Rapport Remediation for Retail-løsningene er IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition en forutsetning.

For IBM Security Trusteer Pinpoint Carbon Copy for Retail er IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition en forutsetning. For IBM Security Trusteer Pinpoint Carbon Copy for Business er IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition eller IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition en forutsetning.

#### 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-løsningene er utformet for å gi et ekstra lag med beskyttelse og en overvåkingstjeneste som kan være til hjelp for å oppdage når en Kvalifisert deltakers legitimasjon er kommet på avveie ved et nettfiskingsangrep på Kundens Retail- eller Business-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for.

#### 3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail skal undersøke, utbedre, blokkere og fjerne infeksjoner med skadelig programvare av typen MitB (Man-in-the-Browser) fra infiserte enheter (PC/MAC) tilhørende Kundens Kvalifiserte deltakere som har tilgang til Kundens Retail-applikasjon, på ad-hoc-basis, der MitB-infeksjoner er oppdaget i hendelsesdata fra IBM Security Trusteer Pinpoint Malware Detection. Kunden må ha et gjeldende abonnement på IBM Security Trusteer Pinpoint Malware Detection som faktisk kjøres på Kundens Retail-applikasjon. Kunden kan bruke denne IBM SaaS-løsningen kun i forbindelse med Kvalifiserte deltakere som har tilgang til Kundens Retail-applikasjon, og kun som et verktøy for å undersøke og utbedre en bestemt infisert enhet (PC/MAC) på ad-hoc-basis. IBM Security Trusteer Rapport Remediation for Retail må faktisk kjøre på en slik berørt Kvalifisert deltakers enhet (PC/MAC), en slik berørt Kvalifisert deltaker må ha akseptert EULA samt være autentisert minst en gang for Kundens Retail-applikasjon(er), og Kundens konfigurasjon må omfatte innsamling av Bruker-IDer. For å unngå tvil, denne IBM SaaS-løsningen omfatter ikke rett til å bruke Trusteer-oppstartsbildet og/eller Klientprogramvaren for kontoinnehavere på noen annen måte enn for Kundens gruppe med Kvalifiserte deltakere.

## 4. IBM Security Trusteer Mobile-løsninger

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

IBM Security Trusteer Mobile Browser er utformet for å gi et ekstra lag med beskyttelse og har som formål å gi sikker online-tilgang for Kvalifiserte deltakeres mobilenheter som får tilgang til Kundens Retail- eller Business-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for, risikovurdering for mobilenheter, samt beskyttelse mot nettfisking. Oppdagelse for sikkert Wi-Fi er bare tilgjengelig for Android-plattformer. For denne IBM SaaS-løsningen omfatter mobilenheter mobiltelefoner og nettbrett, og ikke bærbare PC- og Mac-enheter.

Gjennom TMA kan Kunden (og et ubegrenset antall av Kundens autoriserte personell) motta hendelsesdata, analyser og statistikkinformasjon knyttet til Enheter som tilhører Kvalifiserte deltakere som har (i) lastet ned Klientprogramvaren for kontoinnehavere, en applikasjon med allmenn lisens under en lisensavtale for sluttbrukere ("EULA") vederlagsfri og tilgjengelig for nedlasting til Kvalifiserte deltakeres mobilenheter, og (ii) akseptert EULA og blitt autentisert minst en gang for Kundens Business- eller Retail-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for. Kunden kan bare markedsføre Klientprogramvaren for kontoinnehavere ved bruk av Trusteer-oppstartsbildet, og kan ikke bruke Klientprogramvaren for kontoinnehavere til Kundens interne forretningsoperasjoner.

a. Hendelsesdata:

   Kunden (og et ubegrenset antall av Kundens autoriserte personell) kan bruke TMA til å motta hendelsesdata generert som et resultat av mobilenhetenes online-interaksjoner med Kundens Retail- eller Business-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for.

b. Trusteer-oppstartsbilde:

   Markedsføringsplattformen for Trusteer-oppstartsbildet identifiserer og markedsfører Klientprogramvaren for kontoinnehavere for de Kvalifiserte deltakerne som får tilgang til Kundens Business- og/eller Retail-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for. Kunden kan velge blant tilgjengelige oppstartsbildemaler ("Oppstartsbildemal"). Et tilpasset oppstartsbilde kan avtales under en separat avtale eller tjenestebeskrivelse.

Kunden kan akseptere å fremskaffe sine varemerker, logoer eller ikoner til bruk i forbindelse med TMA og kun til bruk sammen med Trusteer-oppstartsbildet og for visning i Klientprogramvaren for kontoinnehavere eller på landingssider som vertes av IBM, eller på IBM Security Trusteer-nettstedet. Enhver bruk av Kundens avleverte varemerker, logoer eller ikoner vil være i overensstemmelse med IBMs rimelige retningslinjer vedrørende reklame og bruk av varemerker.

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

IBM Security Trusteer Mobile SDK-løsningene er utformet for å gi et ekstra lag med beskyttelse for å gi sikker nettilgang til Kundens Business- og/eller Retail-applikasjoner som Kunden har abonnert på IBM SaaS-dekning for, risikovurdering for enheter, samt beskyttelse mot pharming, også kalt bondephangeri. Oppdagelse for sikkert Wi-Fi er bare tilgjengelig for Android-plattformer.

IBM Security Trusteer Mobile SDK-løsningene omfatter en rettighetsbeskyttet Mobile Software Developer's Kit ("SDK"), en programvarepakke som inneholder dokumentasjon, rettighetsbeskyttede programvarebiblioteker for programmering og andre tilhørende filer og elementer, kjent som IBM Security Trusteer Mobile Library, samt "Kjøretidskomponenten" eller den "Redistribuerbare komponenten", en rettighetsbeskyttet kode generert av IBM Security Trusteer Mobile SDK som kan bygges inn og integreres i Kundens beskyttede frittstående iOS- eller Android-mobilapplikasjoner som Kunden har abonnert på IBM SaaS-dekning for ("Kundens integrerte mobilapp").

IBM Security Trusteer Mobile SDK for Retail er tilgjengelig i pakker på 100 Kvalifiserte deltakere eller pakker på 100 Klientenheter, og IBM Security Trusteer Mobile SDK for Business er tilgjengelig i pakker på 10 Kvalifiserte deltakere eller pakker på 10 Klientenheter.

Gjennom TMA kan Kunden (og et ubegrenset antall av Kundens autoriserte personell) motta hendelsesdatarapporter og risikovurderinger. Gjennom Kundens integrerte mobilapp kan Kunden motta risikoanalyse og mobilenhetsinformasjon knyttet til mobilenhetene til de Kvalifiserte deltakerne som har lastet ned Kundens integrerte mobilapp, slik at det blir mulig for Kunden å formulere en policy for å forhindre svindel og treffe tiltak for å begrense denne risikoen. For denne løsningen omfatter "mobilenheter" bare støttede mobiltelefoner og nettbrett, ikke PC- eller MAC-enheter.

Kunden kan

a. bruke IBM Security Trusteer Mobile SDK internt kun til det formål å utvikle Kundens integrerte mobilapp;

b. innebygge den Redistribuerbare komponenten (kun i objektkodeformat) som en integrert, uatskillelig del av Kundens integrerte mobilapp. Enhver endret eller integrert del av den Redistribuerbare komponenten i overensstemmelse med denne lisenstildelingen skal være underlagt disse Bruksbetingelsene; og

c. markedsføre og redistribuere den Redistribuerbare komponenten for nedlasting til Kvalifiserte deltakeres mobilenheter eller til innehaveren av en Klientenhet, under forutsetning av følgende:

   - Unntatt slik det uttrykkelig er tillatt ifølge denne Avtalen, kan Kunden ikke (1) bruke, kopiere, endre eller distribuere SDK; (2) foreta reversert assemblering eller reversert kompilering av, eller på annen måte oversette eller foreta reversert behandling av SDK utover det som er uttrykkelig tillatt gjennom gjeldende lovgivning uten mulighet for avtalemessige begrensninger; (3) viderelisensiere, leie ut eller lease ut SDK; (4) fjerne filer som inneholder informasjon om opphavsrett eller andre merknader, som finnes i den Redistribuerbare komponenten; (5) bruke samme banenavn som filene/modulene i den opprinnelige Redistribuerbare komponenten; og (6) bruke IBMs, IBMs lisensutstederes eller IBMs distributørers navn eller varemerker i forbindelse med markedsføringen av Kundens integrerte mobilapp uten skriftlig forhåndsgodkjennelse fra IBM eller den aktuelle lisensutstederen eller distributøren.
   - Den Redistribuerbare komponenten må fortsatt være integrert på en uatskillelig måte med Kundens integrerte mobilapp. Den Redistribuerbare komponenten må kun være i objektkodeformat og må overholde alle retningslinjer, instruksjoner og spesifikasjoner i SDK med tilhørende dokumentasjon. Sluttbrukerens lisensavtale for Kundens integrerte mobilapp må informere sluttbrukeren om at den Redistribuerbare komponenten ikke kan i) brukes til noe annet formål enn å aktivere Kundens integrerte mobilapp, ii) kopieres (unntatt for sikkerhetskopiering), iii) videredistribueres eller overføres, iv) behandles med reversert assemblering eller reversert kompilering eller på annen måte oversettes unntatt slik det er

uttrykkelig tillatt ved lov uten mulighet for avtalemessige begrensninger. Kundens lisensavtale må gi IBM like god beskyttelse som betingelsene i denne Avtalen.

- SDK kan bare implementeres som en del av Kundens interne miljø for utvikling og enhetstesting på Kundens spesifiserte mobilenheter for testing. Kunden har ikke rett til å bruke SDK til å behandle produksjonsarbeidsmengder, simulere produksjonsarbeidsmengder eller teste skalerbarhet for kode, applikasjoner eller systemer. Kunden kan ikke bruke noen del av SDK til andre formål.

Kunden er ansvarlig for all teknisk hjelp til Kundens integrerte mobilapp samt alle endringer av de Redistribuerbare komponentene som er utført av Kunden i overensstemmelse med det som tillates her.

Kunden har tillatelse til å installere og bruke de Redistribuerbare komponentene og IBM Security Mobile SDK kun til støtte for Kundens bruk av IBM SaaS-løsningen.

IBM har testet eksempelapplikasjoner som er opprettet ved hjelp av mobilverktøyene som leveres med IBM Security Trusteer Mobile SDK ("Mobilverktøy"), for å avgjøre om de fungerer på riktig måte på bestemte versjoner av mobiloperativsystemplattformer fra Apple (iOS), Google (Android) og andre (samlet kalt "Mobiloperativsystemplattformer"). Mobiloperativsystemplattformer leveres imidlertid av tredjeparter, er derfor ikke under IBMs kontroll, og kan endres uten at IBM blir varslet. IBM garanterer derfor ikke at applikasjoner eller andre utdata som opprettes ved hjelp av Mobilverktøyene, vil fungere på riktig måte på, fungere sammen med eller være kompatible med noen Mobiloperativsystemplattformer eller mobilenheter.

Kunden skal opprette, oppbevare og levere IBM og IBMs revisorer nøyaktige skriftlige registreringer, utdata fra systemverktøy og annen systeminformasjon som er tilstrekkelig for verifisering av at Kundens bruk av IBM Security Trusteer Mobile SDK er i overensstemmelse med disse Bruksbetingelsene.

## 5. Implementering av IBM SaaS Fraud Protection-løsninger

Kundens basisabonnement omfatter nødvendig konfigurering og de første implementeringsaktivitetene, inkludert første engangsoppstart, konfigurering, Oppstartsbildemal, testing og opplæring.

Tilleggstjenester kan avtales mot tilleggsbetaling under en separat avtale.

# Vedlegg B

IBM leverer følgende servicenivåavtale ("Servicenivåavtale" (SLA)) for IBM SaaS, som gjelder hvis den er oppgitt i Kundens Transaksjonsdokument:

Den versjonen av Servicenivåavtalen som er gjeldende ved start eller fornyelse av avtaleperioden for Kundens abonnement, skal gjelde. Kunden er innforstått med at Servicenivåavtalen ikke gir Kunden noen garanti.

## 1. Definisjoner

a. **Autorisert kontaktperson** er den personen Kunden har oppgitt til IBM, og som har fullmakt til å sende inn Krav under denne Servicenivåavtalen.

b. **Avtalemåned** er hver enkelt hele måned i avtaleperioden for IBM SaaS målt fra klokken 00:00 GMT på den første dagen i måneden og til og med klokken 23:59 GMT på den siste dagen i måneden.

c. **Force Majeure** er naturkatastrofer, terrorisme, arbeidsaksjoner, brann, flom, jordskjelv, opptøyer, krig, offentlige påbud, kjennelser eller restriksjoner, virus, tjenestenektangrep og andre skadelige aktiviteter, feil ved strømforsyning og nettverkstilknytning, eller andre årsaker til at IBM SaaS ikke er tilgjengelig, og som er utenfor IBMs kontroll.

d. **Hendelse** er en situasjon eller et sett med situasjoner som sammen fører til en mangel på oppfyllelse av et Servicenivå.

e. **Krav** er et krav som Kundens Autoriserte kontaktperson har sendt til IBM i overensstemmelse med denne Servicenivåavtalen i forbindelse med at et Servicenivå ikke er oppfylt i løpet av en Avtalemåned.

f. **Kunde** er en enhet som abonnerer på IBM SaaS direkte fra IBM, og som ikke er skyldig i mislighold av noen forpliktelser, inkludert betalingsforpliktelser, i henhold til Kundens avtale med IBM om IBM SaaS.

g. **Nedetid** er en periode der produksjonssystembehandlingen for Tjenesten har stoppet, og ingen av Kundens brukere kan bruke noen aspekter av Tjenesten som de har tillatelse til å bruke. Nedetid omfatter ikke perioder der Tjenesten ikke er tilgjengelig på grunn av følgende:

- Planlagt systemnedetid;
- Force Majeure;
- Problemer med Kundens eller tredjeparters applikasjoner, utstyr eller data;
- Handlinger eller mangel på handlinger fra Kundens eller en tredjeparts side (inkludert at noen får tilgang til IBM SaaS ved hjelp av Kundens passord eller utstyr);
- Unnlatelse av å bruke nødvendige systemkonfigurasjoner og støttede plattformer for tilgang til IBM SaaS; eller
- IBMs overholdelse av utforminger, spesifikasjoner eller instruksjoner gitt av Kunden eller av en tredjepart på Kundens vegne.

h. **Planlagt systemnedetid** er en planlagt nedetid for IBM SaaS på grunn av vedlikehold.

i. **Servicenivå** er standarden som er angitt nedenfor, og som IBM måler sitt servicenivå mot for denne Servicenivåavtalen.

j. **Tilgjengelighetskreditering** er den kompensasjonen IBM gir for et godkjent Krav. Tilgjengelighetskrediteringen kan gis i form av en kreditering eller et fradrag mot en fremtidig faktura for abonnementet på IBM SaaS.

## 2. Tilgjengelighetskrediteringer

a. For å kunne sende inn et Krav må Kunden ha logget en problempost for hver Hendelse hos IBMs Help Desk for kundestøtte for den aktuelle IBM SaaS i samsvar med IBMs prosedyre for rapportering av forespørsler om støtte til problemer med alvorsgrad 1. Kunden må oppgi all nødvendig detaljert informasjon om Hendelsen og i rimelig grad hjelpe IBM med å utføre diagnose og finne en løsning for Hendelsen i den grad dette kreves for problemposter med alvorsgrad 1. En slik problempost må være logget innen tjuefire (24) timer etter at Kunden først ble oppmerksom på at Hendelsen påvirket Kundens bruk av IBM SaaS.

b. Kundens Autoriserte kontaktperson må sende Kravet om en Tilgjengelighetskreditering senest tre (3) arbeidsdager etter slutten av Avtalemåneden som Kravet gjelder.

c. Kundens Autoriserte kontaktperson må gi IBM alle detaljer vedrørende Kravet, inkludert, men ikke begrenset til, detaljerte beskrivelser av alle relevante Hendelser og Servicenivået Kunden hevder ikke er oppfylt.

d. IBM skal måle internt den samlede Nedetiden i løpet av hver Avtalemåned som gjelder for tilsvarende Servicenivå vist i tabellen nedenfor. Tilgjengelighetskrediteringer skal baseres på varighet av Nedetid målt fra tidspunktet Kunden rapporterer at Kunden først ble påvirket av Nedetiden. Hvis Kunden rapporterer en Hendelse med Applikasjonsnedetid og en Hendelse med Nedetid for innsamling av innkommende data som skjer samtidig, vil IBM behandle de overlappende periodene med Nedetid som en enkelt periode med Nedetid, og ikke som to separate perioder med Nedetid. For hvert gyldig Krav skal IBM benytte høyeste aktuelle Tilgjengelighetskreditering basert på oppnådd Servicenivå i løpet av hver Avtalemåned som vist i tabellen nedenfor. IBM gir ikke flere Tilgjengelighetskrediteringer for samme Hendelse(r) i samme Avtalemåned.

e. For Pakket Tjeneste (flere IBM SaaS-løsninger pakket og solgt sammen for en samlet pris) blir Tilgjengelighetskrediteringen beregnet basert på den samlede månedlige prisen for den Pakkede Tjenesten, og ikke på den månedlige abonnementsprisen for hver enkelt IBM SaaS. Kunden kan bare sende inn Krav som gjelder en enkelt IBM SaaS i en pakke i en Avtalemåned, og IBM gir ikke Tilgjengelighetskrediteringer for mer enn en enkelt IBM SaaS i en pakke i en Avtalemåned.

f. Hvis Kunden har kjøpt IBM SaaS fra en godkjent IBM-forhandler i en videresalgstransaksjon der IBM beholder hovedansvaret for å oppfylle forpliktelsene vedrørende IBM SaaS og Servicenivåavtalen, blir Tilgjengelighetskrediteringen basert på den gjeldende RSVP-prisen (Relationship Suggested Volume Price) for IBM SaaS på det aktuelle tidspunktet, gjeldende for Avtalemåneden som Kravet gjelder, redusert med 50 %.

g. Samlede Tilgjengelighetskrediteringer for en Avtalemåned skal ikke under noen omstendighet overstige ti prosent (10 %) av en tolvdel (1/12) av det årlige beløpet som Kunden betaler IBM for IBM SaaS.

h. IBM skal bruke rimelig skjønn ved vurderingen av Krav basert på informasjonen som er tilgjengelig i IBMs registreringer, og som skal gjelde hvis det er motstrid mellom dataene i IBMs og Kundens registreringer.

i. TILGJENGELIGHETSKREDITERINGENE SOM GIS KUNDEN I SAMSVAR MED DENNE SERVICENIVÅAVTALEN, ER KUNDENS ENESTE KOMPENSASJON I FORBINDELSE MED ETHVERT KRAV.

## 3. Servicenivåer

Tilgjengelighet av IBM SaaS i løpet av en Avtalemåned

| **Oppnådd Servicenivå (i løpet av en Avtalemåned)** | **Tilgjengelighetskreditering (% av månedlig abonnementspris for Avtalemåneden som Kravet gjelder)** |
|---|---|
| < 99,5 % | 2 % |
| < 98,0 % | 5 % |
| < 96,0 % | 10 % |

"Oppnådd Servicenivå" beregnes prosentvis på følgende måte: (a) totalt antall minutter i en Avtalemåned, minus (b) totalt antall minutter med Nedetid i en Avtalemåned, dividert på (c) totalt antall minutter i en Avtalemåned.

Eksempel: 250 minutter samlet Nedetid i en Avtalemåned

| | |
|---|---|
| 43.200 minutter i en Avtalemåned med 30 dager - 250 minutter Nedetid = 42.950 minutter<br>_____<br>43.200 minutter | = 2 % Tilgjengelighetskreditering for 99,4 % Oppnådd Servicenivå i løpet av Avtalemåneden |

## 3.1 Unntak

Denne Servicenivåavtalen er kun tilgjengelig for IBM-kunder. Denne Servicenivåavtalen gjelder ikke følgende:

- Beta- og prøvetjenester.
- Ikke-produksjonsmiljøer, inkludert men ikke begrenset til miljøer for testing, katastrofehåndtering, kvalitetssikring eller utvikling.
- Krav fra en IBM-kundes brukere, gjester, deltakere og godkjente inviterte som bruker IBM SaaS.
- Hvis Kunden har misligholdt sine forpliktelser i henhold til Bruksbetingelsene, inkludert uten begrensning mislighold av betalingsforpliktelser.