# IBM Application Security on Cloud

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:

- IBM Application Security Analyzer
- IBM Application Security Analyzer Per Scan
- IBM Application Security Analyzer Premium

## 2. Måletyper for betaling

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

a. **Job (Job)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Et Job er et objekt i IBM SaaS-produktet, som ikke kan opdeles yderligere, og som repræsenterer en beregningsproces, inklusive alle underprocesser. Kunden skal anskaffe tilstrækkeligt mange beviser for brugsret til at kunne dække det samlede antal Job, som behandles eller håndteres af IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

b. **Applikationsforekomst (Application Instance)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Der kræves et bevis for brugsret til Applikationsforekomst for hver forekomst af en Applikation, som er knyttet til IBM SaaS-produktet. Hvis en Applikation har flere komponenter, og hver af disse tjener et bestemt formål og/eller en bestemt brugerbasis, og hver af komponenterne kan tilknyttes eller administreres af IBM SaaS-produktet, betragtes hver komponent som en separat Applikation. Derudover betragtes hvert test-, udviklings- og produktionsmiljø for en Applikation som en separat forekomst af Applikationen, og hver forekomst skal være dækket af en brugsret. Flere Applikationsforekomster i et enkelt miljø betragtes som separate forekomster af Applikationen, og hver forekomst skal være dækket af en brugsret. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække det antal Applikationsforekomster, som er tilknyttet IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis på brugsret eller i Transaktionsdokumentet.

c. **Forekomst (Instance)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Ved Forekomst forstås en adgang til en specifik IBM SaaS-konfiguration. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder for hver Forekomst af IBM SaaS-produktet, der stilles til rådighed, til at kunne dække adgang og brug i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

   For hver Forekomst-brugsret gælder det, at der ingen grænse er for antallet af udførte Job eller Applikationsforekomster. Dog kan der ikke udføres mere end 30 job samtidigt på et givet tidspunkt.

## 3. Pris og fakturering

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

### 3.1 Betaling for brug

Serviceydelser med betaling efter forbrug faktureres i den måned, der følger efter anvendelsen af serviceydelsen, og til den pris, der er angivet i Transaktionsdokumentet.

### 3.2 Betaling for del af måned

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

## 4. Varighed og fornyelse

IBM SaaS-perioden begynder den dato, hvor IBM giver Kunden besked om, at Kunden har adgang til IBM SaaS-produktet, som beskrevet i beviset for brugsret. Beviset for brugsret angiver, om IBM SaaS-produktet fornyes automatisk, fortsætter løbende eller ophører ved udgangen af aftaleperioden.

Ved automatisk fornyelse: Medmindre Kunden mindst 90 dage inden periodens udløbsdato informerer IBM om ikke at forny aftaleperioden, fornys IBM SaaS-produktet automatisk for den periode, der er angivet i beviset for brugsret.

Ved løbende brug: IBM SaaS-produktet vil fortsat være tilgængeligt på månedsbasis, indtil Kunden med 90 dages skriftligt varsel til IBM bringer aftalen til ophør. IBM SaaS-produktet vil være tilgængeligt indtil udgangen af den kalendermåned, der følger efter en sådan 90-dages periode.

## 5. Teknisk support

I Abonnementsperioden og efter, at IBM har informeret Kunden om, at Kunden har adgang til IBM SaaS-produktet, leveres teknisk support via onlineforummer og som standardsupport i den periode, hvor Kunden betaler efter forbrug. Kunden kan sende en problemrapport inde fra IBM SaaS eller åbne en chatsession for at få hjælp. IBM stiller IBM Software as a Service Support Handbook til rådighed, som indeholder kontaktoplysninger til brug ved teknisk support og supportprocesser.

| Problemklassificering | Definition af problemklassificering | Målsætning for reaktionstid | Dækning – reaktionstid |
|---|---|---|---|
| 1 | **Funktion/serviceydelse med central indvirkning på forretningen er nede:** En central forretningsfunktion er ude af drift, eller der er fejl på en central grænseflade. Det gælder sædvanligvis et produktionsmiljø og angiver manglende adgang til serviceydelser, hvilket resulterer i en væsentlig påvirkning af driften. Tilstanden kræver en øjeblikkelig løsning. | Inden for 1 time | 24 x 7 |
| 2 | **Betydelig indvirkning på forretningen:** Der er en alvorlig brugsbegrænsning i en forretningsfunktion i serviceydelsen, eller der er risiko for, at tidsfrister ikke overholdes. | Inden for 2 arbejdstimer | Mandag – fredag i arbejdstiden |
| 3 | **Mindre indvirkning på forretningen:** Angiver, at serviceydelsen eller funktioner kan benyttes, og at der ingen alvorlig påvirkning er af driften. | Inden for 4 arbejdstimer | Mandag – fredag i arbejdstiden |
| 4 | **Minimal indvirkning på forretningen:** En forespørgsel eller ikke-teknisk anmodning. | Inden for 1 arbejdsdag | Mandag – fredag i arbejdstiden |

### 5.1 Adgang til kundedata

IBM kan få adgang til kundedata for at identificere problemer med serviceydelsen og for at gøre det nemmere for serviceydelsen at scanne applikationen. IBM tilgår kun data med det formål at rette fejl eller levere support til IBM-produkter eller -serviceydelser.

## 6. Tillægsvilkår for IBM SaaS-produktet

Sikkerhedsscanninger identificerer ikke nødvendigvis alle risici i en applikation.

IBM SaaS-produktet kan bruges til at hjælpe Kunden med at overholde lovgivning, bestemmelser, standarder og praksis. Vejledning, retningslinjer og oplysninger om foreslået brug, der leveres i Serviceydelsen, udgør ikke juridisk, regnskabsmæssig eller anden form for professionel rådgivning, og Kunden tilrådes at indhente sin egen juridiske rådgivning eller ekspertrådgivning. Kunden er eneansvarlig for at sikre, at Kunden og Kundens aktiviteter, applikationer og systemer overholder alle gældende love, bestemmelser, standarder og gældende praksis. Brug af denne Serviceydelse garanterer ikke overholdelse af nogen love, bestemmelser, standarder eller praksis.

IBM SaaS-produktet udfører invasive såvel som ikke-invasive test på det websted og den web- eller mobilapplikation, som Kunden vælger at scanne. En sådan test medfører visse risici, herunder for eksempel:

a. Kundens IT-systemer kan - når applikationer afvikles under test - komme til at hænge eller gå ned, hvorved systemet midlertidigt bliver utilgængeligt, eller data kan gå tabt.

b. Ydeevnen på Kundens systemer og ydeevnen af tilknyttede routere og firewalls kan blive midlertidigt reduceret under testen.

c. Der kan blive genereret mange logmeddelelser, og logfilerne kan optage meget diskplads.

d. Data kan blive ændret eller slettet som følge af undersøgelse af sårbarheder.

e. Systemer til registrering af indtrængen kan udløse alarmer.

f. E-mail kan udløses af e-mailfunktionen i den webapplikation, der testes.

g. IBM SaaS-produktet kan medføre, at trafikken på det overvågede netværk analyseres med henblik på at spore begivenheder.

Hvis Kunden angiver validerede logonoplysninger i Serviceydelsen for den applikation, der testes, skal Kunden kun angive valideringsoplysninger for testkonti, ikke for brugere af produktionssystemet. Brug af valideringsoplysninger for brugere af produktionssystemet kan betyde, at personoplysninger overføres via Serviceydelsen.

IBM SaaS-produktet kan konfigureres til at scanne webapplikationer i produktion. Hvis Kunden angiver scanningstypen til "produktion", er serviceydelsen designet til at scanne på en måde, som mindsker de ovenfor anførte risici. I visse situationer kan IBM SaaS-produktet betyde, at systemets ydeevne reduceres, eller at systemet bliver ustabilt på de testede produktionssteder og den testede infrastruktur. IBM garanterer ikke og fremsætter ingen erklæringer med hensyn til relevansen af at bruge IBM SaaS-produktet til at scanne produktionssteder.

Det er Kundens ansvar at fastslå, om det er fornuftigt eller sikkert i forhold til Kundens websted, webapplikation, mobilapplikation eller Kundens tekniske miljø at benytte Serviceydelsen.

IBM SaaS-produktet er designet til at kunne identificere en lang række mulige sikkerhedsproblemer og problemer med overholdelse af regler og lovgivning i mobile applikationer og webapplikationer og webserviceprogrammer. Det tester ikke alle sårbarheder eller risici i forbindelse med overholdelse af regler og lovgivning, ligesom det heller ikke beskytter mod angreb. Sikkerhedstrusler, bestemmelser og standarder skifter hele tiden, og serviceydelsen afspejler måske ikke alle disse ændringer. Det er alene Kundens ansvar at sørge for, at Kundens webapplikation, systemer og medarbejdere er sikrede og overholder regler og lovgivning, ligesom det alene er Kundens ansvar at træffe afhjælpende foranstaltninger. Det er helt op til Kunden selv at afgøre, om Kunden vil benytte de oplysninger, som Serviceydelsen tilbyder.

Visse love forbyder ethvert uautoriseret forsøg på at trænge ind i et IT-system. Det er Kundens ansvar at sikre, at Kunden ikke benytter Serviceydelsen til at scanne andre websteder og/eller applikationer end websteder og/eller applikationer, som ejes af Kunden, eller som Kunden har ret og autorisation til at scanne.

## 6.2 Cookies

Kunden er opmærksom på og indforstået med, at IBM – som del af den normale drift og support af IBM SaaS-produktet – via sporing eller andre teknologier indsamler personlige informationer fra Kunden (Kundens medarbejdere og kontraktansatte), som vedrører brugen af IBM SaaS-produktet. Det sker for at indsamle brugsstatistik og oplysninger om effektiviteten af IBM SaaS med det formål at forbedre brugeroplevelsen og/eller at skræddersy kommunikationen med Kunden. Kunden bekræfter, at Kunden vil indhente eller har indhentet samtykke til, at IBM kan behandle de indsamlede personoplysninger til ovenstående formål i IBM, andre IBM-virksomheder og disses underleverandører, uanset hvor IBM og IBM's underleverandører driver forretning, og i henhold til gældende lovgivning. IBM vil efterkomme anmodninger fra Kundens medarbejdere og kontraktansatte om adgang til, opdatering, ændring eller sletning af de indsamlede personoplysninger.

## 6.3 Lokaliteter med afledte fordele (Derived Benefit)

Hvor det er relevant, baseres skatter og afgifter på den eller de lokationer, Kunden identificerer som værende den eller de lokationer, der modtager fordelen ved IBM SaaS-produktet. IBM inkluderer skatter og afgifter på basis af den forretningsadresse, Kunden anfører som primær fordelslokalitet ved bestilling

af et IBM SaaS-produkt, medmindre Kunden informerer IBM om andet. Det er Kundens ansvar at sørge for, at oplysningerne er opdateret og at informere IBM om eventuelle ændringer.

# Bilag A

## 1. Generel beskrivelse af IBM Application Security on Cloud

IBM Application Security on Cloud tilbyder ét centralt sted, hvor Kunden kan få hjælp til at identificere sikkerhedssårbarheder (f.eks. SQL Injection, Cross-Site Scripting og Data Leakage) for forskellige applikationer. Serviceydelsen inkluderer forskellige teknikker til sikkerhedsscanning af applikationer, og hver tekniktype identificerer sikkerhedsproblemer i den specifikke applikation.

IBM Application Security on Cloud tilbyder følgende faciliteter:

- Scanning af mobilapplikationer for sikkerhedssårbarheder. Det sker via teknikker til dynamisk (blackbox) og interaktiv (glassbox) sikkerhedsanalyse.
- Scanning af produktions- og præproduktionswebsteder, netværk vendt mod offentligheden eller private netværk og scanning af websteder for sikkerhedssårbarheder. Det sker via en teknik til dynamisk (blackbox) sikkerhedsanalyse.
- Scanning af datastrømme i web- og skrivebordsapplikationer for sikkerhedssårbarheder. Det sker via en teknik til statisk (whitebox) sikkerhedsanalyse.
- Detaljerede rapporter om sikkerhedssårbarheder, som både inkluderer overordnede oversigter over resultaterne og en beskrivelse af, hvad udviklerne kan gøre for at afhjælpe sårbarhederne.
- Integrering med forskellige DevOps-platforme.