IBM Application Security on Cloud

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 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:

- IBM Application Security Analyzer

2. Målenheter for omkostninger

IBM SaaS selges under en av følgende målenheter for omkostninger som spesifisert i Transaksjonsdokumentet:

a. **Applikasjonsforekomst** (Application Instance) er en målenhet for anskaffelse av IBM SaaS. Det kreves en Applikasjonsforekomst-rettighet for hver forekomst av en Applikasjon som er koblet til IBM SaaS. Hvis en Applikasjon har flere komponenter som hver tjener et særskilt formål og/eller brukerbase, og som hver kan kobles til eller administreres av IBM SaaS, anses hver slik komponent som en separat Applikasjon. Dessuten anses hvert test-, utviklings-, opprioriterings- og produksjonsmiljø for en Applikasjon som en separat forekomst av Applikasjonen, og må ha en rettighet. Flere Applikasjonsforekomster i ett enkelt miljø anses også som egne forekomster av Applikasjonen, og hver forekomst må ha en rettighet. Det må anskaffes tilstrekkelig antall rettigheter for å dekke antall Applikasjonsforekomster som er koblet til IBM SaaS i løpet av måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

b. **Tilgang** (Access) er en målenhet for anskaffelse av IBM SaaS. En Tilgang gir rett til å bruke IBM SaaS. Kunden må anskaffe en enkelt Tilgang-rettighet for å kunne bruke IBM SaaS i måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

3. Priser og fakturering

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

3.1 Betaling per bruk (Pay per Use)

Pay per Use-alternativer blir fakturert i den påfølgende måneden etter at tjenesten er benyttet, til prisen som er angitt i Transaksjonsdokumentet.

3.2 Pris for del av måned

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

4. Teknisk støtte

I Abonnementsperioden og etter at IBM har varslet Kunden om at tilgangen til IBM SaaS er tilgjengelig, gis teknisk støtte via online-fora og som Standard-støtte i den perioden Kunden betaler Pay per Use-beløp for. Fra IBM SaaS kan Kunden sende en problemrapport eller åpne en nettsamtalesesjon for å be om hjelp. IBM vil gjøre IBM Software as a Service Support Handbook tilgjengelig for Kunden, og denne håndboken inneholder kontaktinformasjon for teknisk støtte samt informasjon om prosesser og annen informasjon.

Alvorsgrad	Definisjon av alvorsgrad	Mål for kontakttid	Dekningstid
1	**Kritisk virkning på forretningsdriften/tjeneste nede:** Virksomhetskritiske funksjoner er ikke i driftsmessig stand eller et viktig grensesnitt fungerer ikke. Dette gjelder vanligvis et produksjonsmiljø og indikerer en mangel på tilgang til tjenester, noe som har kritisk innvirkning på driften. Denne situasjonen krever en umiddelbar løsning.	Innen 1 time	24x7
2	**Betydelig virkning på forretningsdriften:** En forretningsfunksjon eller funksjon i tjenesten har betydelig begrenset bruksmulighet eller Kunden står i fare for å ikke nå sine tidsfrister.	Innen 2 timer i arbeidstiden	M-F i arbeidstiden
3	**Liten virkning på forretningsdriften:** Angir at tjenesten eller funksjonen kan brukes, og at den ikke har en kritisk virkning på driften.	Innen 4 timer i arbeidstiden	M-F i arbeidstiden
4	**Minimal virkning på forretningsdriften:** Et spørsmål eller en forespørsel som ikke er av teknisk art	Innen 1 arbeidsdag	M-F i arbeidstiden

4.1 Tilgang til Kundens data

IBM har tilgang til Kundens data for å kunne utføre diagnose av problemer med tjenesten og for tjenestens avsøking av Kundens applikasjon. IBMs tilgang til dataene gjelder kun når formålet er å rette feil eller gi støtte for IBMs produkter eller tjenester.

5. Tilleggsbetingelser for IBM SaaS

Det er mulig at sikkerhetssøk ikke identifiserer all sikkerhetsrisiko i en applikasjon.

IBM SaaS kan hjelpe Kunden med å overholde Kundens forpliktelser, basert på lover, forskrifter, standarder og retningslinjer. Anvisninger, forslag til bruk eller veiledning fra Tjenesten utgjør ikke juridiske, regnskapsmessige eller andre faglige råd, og Kunden anbefales å søke juridisk bistand eller annen eksperthjelp. Kunden er alene ansvarlig for å sørge for at Kunden og Kundens aktiviteter, applikasjoner og systemer er i samsvar med alle gjeldende lover, forskrifter, standarder og retningslinjer. Bruk av denne Tjenesten garanterer ikke overholdelse av lovgivning, forskrifter, standarder eller retningslinjer.

IBM SaaS utfører angrepstester og ikke-angrepstester på nettstedet og web- eller mobilapplikasjonen Kunden velger å avsøke, og disse testene er beheftet med en viss risiko, inkludert uten begrensning følgende:

a. Kundens datasystemer som kjører applikasjoner under en test, kan henge eller krasje, noe som kan føre til at systemet blir midlertidig utilgjengelig, eller til tap av data;

b. ytelse og hastighet for Kundens systemer, samt ytelse og hastighet for tilknyttede rutere og brannmurer, kan reduseres midlertidig under tester;

c. det kan genereres store mengder loggmeldinger, noe som fører til stort forbruk av diskplass for loggfiler;

d. data kan bli endret eller slettet ved undersøkelser av sårbarhet;

e. alarmer fra innbruddspåvisningssystemer kan utløses;

f. sending av e-poster kan utløses av e-postfunksjonen i webapplikasjonen som testes;

og

g. skytjenesten kan fange opp trafikken i det overvåkede nettverket med formål å se etter hendelser.

Dersom Kunden oppgir autentisert påloggingslegitimasjon i Tjenesten for applikasjonen som testes, må Kunden bare oppgi slik legitimasjon for testkontoer, ikke for produksjonsbrukere. Bruk av produksjonsbrukerlegitimasjon kan føre til at personlige data overføres via Tjenesten.

IBM SaaS kan konfigureres for å avsøke produksjonswebapplikasjoner. Hvis Kunden angir avsøkingstypen som "produksjon", er tjenesten utformet for å utføre søk på en måte som reduserer risikoen beskrevet ovenfor, men i enkelte situasjoner kan Skytjenesten føre til redusert ytelse eller stabilitet innenfor produksjonssteder og infrastruktur som testes. IBM gir ingen garantier eller løfter vedrørende velegnethet av Skytjenesten for avsøking av produksjonssteder.

DET ER KUNDENS ANSVAR Å AVGJØRE OM TJENESTEN ER PASSENDE ELLER SIKKER FOR KUNDENS NETTSTED, WEBAPPLIKASJON, MOBILAPPLIKASJON ELLER TEKNISKE MILJØ.

IBM SaaS er utformet for å identifisere en rekke potensielle sikkerhets- og overholdelsesproblemer i mobil- og webapplikasjoner og webtjenester. Tjenesten tester ikke for all sårbarhets- eller overholdelsesrisiko, og fungerer heller ikke som en sperre for sikkerhetsangrep. Sikkerhetstrusler, forskrifter og standarder endres kontinuerlig, og det er ikke sikkert at Tjenesten reflekterer alle slike endringer. Sikkerhet og overholdelse knyttet til Kundens webapplikasjon, systemer og ansatte, samt alle avhjelpende tiltak, er Kundens forpliktelse. Kunden velger etter eget skjønn om informasjonen som leveres av Tjenesten, skal benyttes eller ikke.

Lovgivningen kan inneholde bestemmelser som forbyr uautoriserte forsøk på å bryte seg inn i eller få tilgang til datamaskinsystemer. KUNDEN ER ANSVARLIG FOR Å KONTROLLERE AT KUNDEN IKKE BRUKER TJENESTEN TIL Å AVSØKE NOEN ANDRE NETTSTEDER OG/ELLER APPLIKASJONER ENN NETTSTEDER OG/ELLER APPLIKASJONER SOM KUNDEN EIER ELLER SOM KUNDEN HAR RETT OG TILLATELSE TIL Å AVSØKE.

5.2 Informasjonskapsler (cookies)

Kunden er innforstått med og aksepterer at IBM som en del av normal drift og støtte for IBM SaaS kan samle inn personopplysninger fra Kunden (Kundens ansatte og kontraktører) knyttet til bruken av IBM SaaS, gjennom sporing og andre typer teknologi. IBM gjør dette for å samle inn bruksstatistikk og informasjon om hvor effektivt IBM SaaS er, med formål å forbedre brukeropplevelsen og/eller tilpasse interaksjonen med Kunden. Kunden bekrefter at Kunden skal innhente eller har innhentet samtykke til at IBM kan behandle de innsamlede personopplysningene for formålet beskrevet ovenfor, innenfor IBM, andre IBM-selskaper og deres underleverandører, der IBM og IBMs underleverandører driver virksomhet, i henhold til gjeldende lovgivning. IBM skal etterkomme forespørsler fra Kundens ansatte og kontraktører om tilgang til og oppdatering, retting eller sletting av deres innsamlede personopplysninger.

5.3 "Derived Benefit Locations"

Der det er aktuelt, er skatter og avgifter basert på steder der Kunden oppgir å dra fordel av IBM SaaS. IBM skal benytte skatter og avgifter basert på forretningsadressen som er oppgitt ved bestilling av en IBM SaaS-løsning, som primært fordelssted (primary benefit location), med mindre Kunden oppgir annen informasjon til IBM. Kunden er ansvarlig for å holde slik informasjon oppdatert, og informere IBM om eventuelle endringer.

Vedlegg A

1. Generell beskrivelse av IBM Application Security on Cloud

IBM Application Security on Cloud gir et sentralt sted der Kunden kan få hjelp til å identifisere sikkerhetssårbarhet (som SQL-injeksjon, skripting på tvers av websteder (XSS) og datalekkasje) for ulike applikasjoner. Tjenesten omfatter forskjellige typer av avsøkingsteknikker for applikasjonssikkerhet, som hver identifiserer sikkerhetsproblemer i den aktuelle applikasjonen.

IBM Application Security on Cloud omfatter følgende funksjonalitet:

- Avsøking av mobilapplikasjoner for sikkerhetssårbarhet. Dette utføres via teknikker for dynamisk (blackbox) og interaktiv (glassbox) sikkerhetsanalyse.
- Avsøking av produksjons- og førproduksjonsnettsteder for sikkerhetssårbarhet. Dette utføres via teknikker for dynamisk (blackbox) sikkerhetsanalyse.
- Avsøking av dataflyter innenfor web- og skrivebordsapplikasjoner for sikkerhetssårbarhet. Dette utføres via teknikker for statisk (whitebox) sikkerhetsanalyse.
- Detaljerte rapporter om sikkerhetssårbarhet, som omfatter både sammendrag av funnene og fremgangsmåter for utbedring som utviklere kan følge.
- Integrering med forskjellige DevOps-plattformer, som Maven og IBM UrbanCode