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 de Generelle betingelsene. 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
- IBM Application Security on Cloud Consulting Services

2. Målenheter for omkostninger

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

a. **Jobb** (Job) er en målenhet for anskaffelse av IBM SaaS. En Jobb er et objekt i IBM SaaS som ikke kan deles opp ytterligere, og som representerer en databehandlingsprosess inkludert dens underprosesser. Det må anskaffes tilstrekkelig antall rettigheter for å dekke totalt antall Jobber som behandles eller administreres av IBM SaaS i løpet av måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

b. **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.

   For denne IBM SaaS-løsningen gjelder følgende:

   - For dynamisk testing: et nettsted som er adresserbart via offentlig eller privat URL. Hver Applikasjonsforekomst har rett til et nettsted på inntil 1.000 sider i ett enkelt domene.
   - For statisk testing: en utførbar kodeenhet i ett enkelt programmeringsspråk. Hver Applikasjonsforekomst har rett til avsøking av kodeenheter på inntil 1.000.000 linjer.
   - For mobiltesting: en binærkodeenhet som kan utføres på en mobilenhet. Hver mobilplattform (f.eks. iOS og Android) utgjør forskjellige Applikasjonsforekomster.

c. **Forekomst** (Instance) er en målenhet for anskaffelse av IBM SaaS. En Forekomst er tilgang til en bestemt konfigurasjon av IBM SaaS. Det må anskaffes tilstrekkelig antall rettigheter for hver Forekomst av IBM SaaS som gjøres tilgjengelig for tilgang og bruk i løpet av måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

   For hver Forekomst-rettighet er det ingen grense for antall Jobber som utføres, eller antall Applikasjonsforekomster (Applikasjoner tilkoblet), under den forutsetning at maksimalt 30 Jobber kan kjøre samtidig på et gitt tidspunkt.

d. **Engasjement** (Engagement) er en målenhet for anskaffelse av tjenestene. Et Engasjement består av spesialist- og/eller opplæringstjenester knyttet til IBM SaaS. Det må anskaffes tilstrekkelig antall rettigheter for å dekke hvert Engasjement.

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.

3.2 Priser for ekstra volum

Hvis faktisk bruk av IBM SaaS i måleperioden overstiger rettighetene som er oppgitt i Kjøpsbeviset (PoE), blir Kunden fakturert for slikt ekstra volum i samsvar med det som er oppgitt i Transaksjonsdokumentet.

3.3 Priser for oppsett

Kunden blir fakturert for oppsett slik det er oppgitt i Transaksjonsdokumentet.

4. Alternativer for avtaleperiode og fornyelse

Avtaleperioden for IBM SaaS starter den dagen IBM varsler Kunden om at Kunden har tilgang til IBM SaaS, som beskrevet i Kjøpsbeviset. Kjøpsbeviset angir om IBM SaaS-abonnementet fornyes automatisk, løper videre eller opphører ved slutten av avtaleperioden.

Ved automatisk fornyelse er det slik at hvis Kunden ikke minst 30 dager før utløpsdatoen for avtaleperioden sender et skriftlig varsel om at Kunden ikke ønsker fornyelse, blir IBM SaaS-abonnementet fornyet automatisk for avtaleperioden som er angitt i Kjøpsbeviset.

Ved fortløpende bruk vil IBM SaaS fortsette å være tilgjengelig på månedsbasis til Kunden sender et 30 dagers skriftlig forhåndsvarsel om oppsigelse. IBM SaaS fortsetter å være tilgjengelig til slutten av kalendermåneden etter en slik periode på 30 dager.

5. 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

5.1 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.

6. Tilleggsbetingelser for IBM SaaS

Det er mulig at sikkerhetssøk ikke identifiserer all sikkerhetsrisiko i en applikasjon, og de er heller ikke utformet for eller beregnet på bruk i farlige miljøer som krever feilsikker drift, inkludert uten begrensning flynavigeringssystemer, flytrafikkontrollsystemer, våpensystemer, respiratorer, kjernekraftverk eller andre applikasjoner der manglende identifisering av sikkerhetsrisiko kan føre til død, personskade eller skade på eiendom. Sikkerhetssøk er ikke garantert å fungere uten avbrudd eller feilfritt.

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. Lovgivningen kan inneholde bestemmelser som forbyr uautoriserte forsøk på å bryte seg inn i eller få tilgang til datamaskinsystemer. Kunden gir IBM tillatelse til å utføre Tjenestene slik det er beskrevet i dette dokumentet, og bekrefter at Tjenestene innebærer autorisert tilgang til Kundens datamaskinsystemer. IBM kan gjøre denne tillatelsen kjent for en tredjepart hvis det anses som nødvendig for å kunne utføre Tjenestene.

Testingen 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;

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

Alle rettigheter eller beføyelser gitt av IBM i en servicenivåavtale og knyttet til nettstedene eller applikasjonene som testes, fraskrives under testingen.

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 IBM SaaS føre til redusert ytelse eller stabilitet innenfor produksjonssteder og infrastruktur som testes. IBM gir ingen garantier eller løfter vedrørende velegnethet av IBM SaaS 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.

Det understrekes at Kundens innhold som er beskrevet i punktet om beskyttelse av personopplysninger i IBM Bruksbetingelser – Generelle betingelser, også anses å omfatte data som kan bli tilgjengelige for IBM under applikasjonspenetreringstesting.

6.1 Systemer eid av en tredjepart

For systemer (som i denne bestemmelsen omfatter, men ikke er begrenset til, applikasjoner og IP-adresser) eid av en tredjepart, som vil være objekt for testingen som utføres under disse Bruksbetingelsene, aksepterer Kunden

a. at før IBM starter testing av et tredjepartssystem, skal Kunden innhente et undertegnet dokument fra eieren av hvert system, som gir IBM tillatelse til å utføre Tjenestene på det systemet, og som angir eierens aksept av betingelsene som fremkommer i punktet "Permission to Perform Testing", samt gi IBM en kopi av en slik tillatelse;

b. å alene være ansvarlig for å informere systemeieren om eventuell risiko, eksponering og sårbarhet som blir oppdaget på disse systemene ved IBMs eksterne testing; og

c. å legge til rette for utveksling av informasjon mellom systemeieren og IBM slik IBM anser det som nødvendig.

Kunden skal

- umiddelbart informere IBM når det skjer en endring i eierskapet for et av systemene som er objekt for testingen som utføres under disse Bruksbetingelsene;
- ikke gjøre kjent leveransene, eller at IBM utførte Tjenestene, utenfor Kundens Konsern uten skriftlig forhåndsgodkjennelse fra IBM; og
- ivareta interessene til og holde IBM skadesløs overfor tap eller ansvar som påføres IBM på grunn av krav fra tredjepart, som skyldes at Kunden ikke har overholdt betingelsene i dette punktet "Systemer eid av en tredjepart", samt overfor stevninger eller krav fra tredjepart mot IBM eller IBMs underleverandører eller agenter, som skyldes (a) testing av sikkerhetsrisiko, eksponering eller sårbarhet hos systemene som er objekt for testing under disse Bruksbetingelsene, (b) overlevering av resultatene av slik testing til Kunden, eller (c) Kundens bruk eller avgivelse av slike resultater.

6.2 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.

Som en del av IBM SaaS som omfatter rapporteringsaktiviteter, skal IBM klargjøre og vedlikeholde deidentifisert og/eller aggregert informasjon samlet inn fra IBM SaaS (kalt "Sikkerhetsdata"). Sikkerhetsdataene skal ikke identifisere Kunden eller en enkelt person, unntatt som angitt i (d) nedenfor. Kunden aksepterer dessuten at IBM kan bruke og/eller kopiere Sikkerhetsdataene kun for å

a. publisere og/eller distribuere Sikkerhetsdataene (f.eks. i kompileringer og/eller analyser knyttet til cybersikkerhet);

b. utvikle eller forbedre produkter eller tjenester;

c. drive forskning internt eller sammen med tredjeparter; og

d. utføre lovlig deling av informasjon vedrørende bekreftede tredjepartsgjerningsmenn.

6.3 "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.

6.4 Personopplysninger, lovregulert innhold og tjenester

Denne IBM SaaS-løsningen er ikke utformet i henhold til bestemte sikkerhetskrav for lovregulert innhold, som personopplysninger eller sensitive personopplysninger. Kunden er ansvarlig for å avgjøre om denne IBM SaaS-løsningen oppfyller Kundens behov knyttet til typen innhold Kunden bruker i forbindelse med IBM SaaS.

IBM opererer ikke som en leverandør av tjenester som er regulert av US Federal Communications Commission ("FCC") eller amerikanske delstaters reguleringsmyndigheter ("Delstatsmyndigheter"), og har ikke til hensikt å levere noen tjenester som er regulert av FCC eller Delstatsmyndigheter. Hvis FCC eller en Delstatsmyndighet pålegger lovbestemte krav på tjenester som IBM leverer under disse Bruksbetingelsene, kan IBM (a) endre, bytte ut eller erstatte produkter på Kundens bekostning, og/eller (b) endre måten slike tjenester leveres til Kunden på, for å unngå at slike krav eller forpliktelser pålegges IBM (for eksempel ved å fungere som Kundens agent for å skaffe slike tjenester fra en tredjeparts teleleverandør).

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, allment tilgjengelige eller i private nettverk, 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.

1.1 IBM Application Analyzer

IBM Application Analyzer kan bestilles per Applikasjonsforekomst, per Jobb (avsøking) eller som en fullstendig Forekomst, og muliggjør følgende typer av avsøking:

- Dynamic Analyzer – Testing av preproduksjons- eller produksjonsnettsteder via DAST-teknikker
- Mobile Analyzer – Testing av iOS- eller Android-binærfiler via IAST-teknikker
- Static Analyzer – Testing av byte- eller kildekodedataflyt via SAST-teknikker

1.2 Oppsettjenester

IBM Application Security on Cloud Consulting Services er en oppsettjeneste for Application Analyzer. Tjenesten benytter IBM-konsulenter som gir veiledning og assistanse med testing og håndtering av applikasjonsrisiko. IBM Application Security on Cloud Consulting Services anskaffes i form av blokker med Engasjementer som kan benyttes i antallene angitt nedenfor, til forespørsler om og bruk av følgende tjenester:

a. **Fast Start** [Bruker en (1) Engasjement-enhet]

Fast Start-tjenesten gir ekspertise og veiledning for bruk av Application Security on Cloud-funksjonene for testing og riskikostyring. Etter at Kunden har bekreftet vellykket pålogging til Application Security on Cloud-portalen, avholder IBM en webkonferanse på inntil to (2) timer og for inntil to (2) aktive deltakere for å gi opplæring i grunnleggende AppSec-konfigurasjoner og -funksjoner i IBM SaaS, inkludert avsøkingstyper, kjøring av avsøkinger, gjennomgang av rapporter og installering av tilknyttede verktøy og plugin-moduler. Fast Start-tjenesten er fullført når følgende er fullført: (a) Kundens opplæringswebinar, (b) installering av aktuelle verktøy og plugin-moduler, og (c) hjelp til Kunden med oppsett og kjøring av Kundens første avsøking.

b. **Assessment Review** [Bruker to (2) Engasjement-enheter]

Assessment Review-tjenesten gir hjelp til gjennomgang av et testresultat, inkludert forståelse og prioritering av fremgangsmåter for utbedring av sårbarhet i applikasjonen. IBM avholder en webkonferanse på inntil en (1) time og for inntil to (2) aktive deltakere for å gi en oversikt over sårbarhet som er funnet, og samlet sikkerhetsrisiko for applikasjonen samt en detaljert diskusjon av applikasjonens sikkerhetssårbarhet, inkludert (1) hvordan sårbarhet ble testet, (2) hvordan sårbarhet ble oppdaget, (3) hver enkelt sårbarhets risiko, og (4) generelle anbefalinger for hvordan sårbarheten kan utbedres. Gjennomgangen vil være basert kun på testresultatene og vil ikke være en gjennomgang av selve kildekoden. Kunden ser gjennom testresultatene og angir for IBM hvilke testresultater som ønskes gjennomgått, før webkonferansen. Assessment Review-tjenesten er fullført når webkonferansen er gjennomført.

c. **Scan for Me** [Bruker fire (4) Engasjement-enheter]

Scan for Me-tjenesten gir en IBM-ekspert på applikasjonssikkerhet som konfigurerer og kjører en avsøking, validerer resultatene og avholder en rapportorientering for å gjennomgå funnene. Kunden gir en IBM-konsulent tilgang til Kundens ASoC-miljø, som konfigurerer og kjører en avsøking, validerer resultatene, gir anbefalinger vedrørende prioritering av utbedring, og avholder en rapportorientering vedrørende resultatene. IBM avholder en webkonferanse på inntil en (1) time og for inntil to (2) aktive deltakere for å gi en oversikt over sårbarhet som er funnet, og samlet sikkerhetsrisiko for applikasjonen samt en detaljert diskusjon av applikasjonens sikkerhetssårbarhet, inkludert (1) hvordan sårbarhet ble testet, (2) hvordan sårbarhet ble oppdaget, (3) hver enkelt sårbarhets risiko, og (4) generelle anbefalinger for hvordan sårbarheten kan utbedres. På forespørsel, og inntil 30 dager etter den første avsøkingen, kan IBM utføre en ny avsøking basert på den opprinnelige avsøkingskonfigurasjonen, kun for å verifisere sikkerhetsrettelser, ikke for å teste ny funksjonalitet, validere resultater og levere en rapport til Kunden. Scan for Me-tjenesten er fullført når webkonferansen for å gjennomgå de første avsøkingsresultatene er gjennomført, eller, hvis aktuelt, når en ny avsøking forespurt av Kunden er gjennomført og ny avsøkingsrapport er avlevert Kunden.

d. **Advisor on Demand** [Bruker sju (7) Engasjement-enheter]

Advisor on Demand-tjenesten gir inntil tjue (20) timer med konsulenttid fra en IBM-konsulent, som kan brukes til aktiviteter knyttet til IBM SaaS. IBM-konsulenten hjelper Kunden med emner knyttet til applikasjonssikkerhet, inkludert, men ikke begrenset til, programadministrasjon, prioritering av sikkerhetstesting, strategier for utbedring, samt analyse og reparasjon av kildekode. IBM vil samarbeide med Kunden om å forstå og opprette en prosjektplan med Kundens spesifikke behov, inkludert prosjektmål, relevante teknologier, ønskede tidslinjer, forventede leveranser, samt et estimert antall Advisor on Demand-tjenesteengasjementer. Kunden må gi tilgang til applikasjoner, systemer og dokumentasjon som er nødvendige for å kunne utføre tjenesten. Advisor on Demand-tjenesten er fullført når inntil 20 timer med sikkerhetsekspertise er utført og/eller prosjektplanen og/eller dokumenterte leveranser som er definert i prosjektplanen, er levert til Kunden.

e. **Applikasjonspenetreringstesting**

Tre alternativer:

(1) **Compliance/Entry-Level Application Penetration Test**, som omfatter inntil førti (40) timer med konsulenttid, og fokuserer på logiske feil av typen "Single-step logic flaws" og enklere versjoner av "injection flaws". Bruker femten (15) Engasjement-enheter.

(2) **Standard Application Penetration Test**, som omfatter inntil seksti (60) timer med konsulenttid, og utvider fokus for å inkludere logiske feil av typen "Logic flaws in multi-step work flows", komplekse versjoner av "injection flaws" samt analyse av komplekse datatyper. Bruker tjueen (21) Engasjement-enheter.

(3) **Advanced Application Penetration Test**, som omfatter inntil åtti (80) timer med konsulenttid, og utvider fokus for å inkludere reversert utvikling av kompilerte utførbare filer, disseksjon av tilpassede nettverksprotokoller, samt dybdeanalyse av allment tilgjengelige biblioteker og rammeverk. Bruker tjuesju (27) Engasjement-enheter.

Tjenesten for applikasjonspenetreringstesting gir en IBM-ressurs som skal utføre testing og utnyttelse av en applikasjon, levering av en testrapport, samt en orientering om rapporten som forklarer funnene og tilknyttet risiko.

IBM avholder en telefonkonferanse ved prosjektoppstart på inntil en (1) time og for inntil to (2) aktive deltakere for å gjennomgå Kundens miljø og organisasjon, inkludert applikasjonsplattform, arkitektur, rammeverk, støtteinfrastruktur, kjente eller mulige sikkerhetsproblemer knyttet til applikasjonen, foreløpig testplan og plan for kontaktpersoner ved nødsituasjoner.

IBM gjennomfører applikasjonspenetreringstestingen, inkludert, men ikke begrenset til, følgende: identifikasjon av generell sårbarhet som SQL-injeksjon og skripting på tvers av websteder (XSS), vurdering av styrker og svakheter ved eksisterende sikkerhetskontroller som inndatavalidering, autentisering og autorisasjon, kontroll av egnet håndheving av forretningslogikk, validering av egnet bruk av sikkerhetsprotokoller, identifisering av sesjonshåndteringsfeil samt verifisering av egnede sikkerhetskontroller for pålogging, gjenoppretting av passord, passordpolicy og andre funksjoner for brukeradministrasjon. Funn blir dokumentert i rapporten Application Penetration Test Report. IBM avholder en webkonferanse for orientering om rapporten på inntil en (1) time. Application

Penetration Test-tjenesten er fullført når tildelt konsulenttid er brukt opp, webkonferansen er gjennomført, og endelig Application Penetration Test Report er levert Kunden.

1.2.1 Forpliktelser ved oppsettjenester

IBM skal

- levere oppsettjenester ved bruk av Engasjement-enheter anskaffet av Kunden, samt ifølge Kjøpsbeviset (PoE); og
- ha fullført oppsettjenestene når fullførelseskriteriene som er beskrevet i punkt 1.2, er fullført.

Kunden aksepterer

- å være ansvarlig for alle beløp knyttet til alle forespørsler om Engasjement fra Kunden i løpet av avtaleperioden;
- og erkjenner at anskaffede Engasjement-enheter må brukes opp innen den første avtaleperioden samt at de utløper hvis de ikke er brukt ved sluttdatoen for avtaleperioden; og
- å sende en formell forespørsel for alle oppsettjenester minst 30 dager før sluttdatoen for abonnementet.

I forbindelse med utførelsen av en oppsettjeneste kan IBM be Kunden om informasjon og rimelig samarbeid. Hvis Kunden ikke innen rimelig tid har fremskaffet forespurt informasjon, kan det etter IBMs eget skjønn føre til belastning av Engasjement-enheter som er nødvendige på grunn av tjenestene eller forsinkelser i utførelsen av den aktuelle tjenesten.

For at IBM skal kunne gjennomføre en nøyaktig testing, aksepterer Kunden å følge IBMs instruksjoner for klargjøring og vedlikehold av miljøet i testperioden.