IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding

IBM Application Security on Cloud

De Gebruiksvoorwaarden ("ToU") bestaan uit deze IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding ("SaaS Specifieke Voorwaarden voor Aanbieding") en een document met de titel IBM Gebruiksvoorwaarden – Algemene bepalingen ("Algemene Voorwaarden") dat beschikbaar is op de volgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In geval van tegenstrijdigheid prevaleren de SaaS Specifieke Voorwaarden voor Aanbieding boven de Algemene Voorwaarden. Door de IBM SaaS te bestellen, te openen of te gebruiken, geeft Klant aan akkoord te gaan met de Gebruiksvoorwaarden.

De Gebruiksvoorwaarden worden beheerst door de IBM International Passport Advantage Overeenkomst, de IBM International Passport Advantage Express Overeenkomst of de IBM International Agreement for Selected IBM SaaS Offerings, zoals van toepassing ("Overeenkomst") en vormen samen met de Gebruiksvoorwaarden de volledige overeenkomst.

1. IBM SaaS

De volgende IBM SaaS-aanbiedingen worden gedekt door deze SaaS Specifieke Voorwaarden voor Aanbieding:

- IBM Application Security Analyzer

2. Maateenheden voor verschuldigde bedragen

De IBM SaaS wordt verkocht onder de volgende maateenheden voor verschuldigde bedragen, zoals gespecificeerd in het Transactiedocument:

a. **Applicatie Instance** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Er is een Applicatie Instance gebruiksrecht vereist voor elke instance van een Applicatie die verbonden is met de IBM SaaS. Indien een bepaalde Applicatie meerdere componenten heeft, elk daarvan een specifiek doel dient en/of een specifieke gebruikersbasis bedient, en elk daarvan kan worden verbonden met of beheerd door de IBM SaaS, wordt elke dergelijke component beschouwd als een afzonderlijke Applicatie. Bovendien worden test-, ontwikkelings-, staging- of productieomgevingen voor een Applicatie beschouwd als afzonderlijke instances van de Applicatie en is er voor elk daarvan een gebruiksrecht vereist. Meerdere instances van een Applicatie in een enkele omgeving worden beschouwd als afzonderlijke instances van de Applicatie en is er voor elk van die instances een gebruiksrecht vereist. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van het aantal Applicatie Instances dat met de IBM SaaS is verbonden tijdens de meetperiode zoals aangegeven in het Bewijs van Gebruiksrecht of Transactiedocument van Klant.

b. **Toegang** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Toegang is het recht om gebruik te maken van de IBM SaaS. Klant dient een enkel gebruiksrecht voor Toegang te verkrijgen om tijdens de meetperiode zoals aangegeven in het Bewijs van Gebruiksrecht of Transactiedocument van Klant, gebruik te mogen maken van de IBM SaaS.

3. Verschuldigde bedragen en facturering

Het verschuldigde bedrag voor de IBM SaaS wordt aangegeven in een Transactiedocument.

3.1 Betaling per Gebruik

Opties voor Betaling per Gebruik (Pay per Use) worden in de maand die volgt op de maand waarin de service is gebruikt, gefactureerd tegen het in het Transactiedocument gespecificeerde tarief.

3.2 Verschuldigd bedrag voor een deel van een maand

Voor een deel van een maand kunnen er pro rato verschuldigde bedragen in rekening worden gebracht, zoals gespecificeerd in het Transactiedocument.

4. Technische ondersteuning

Nadat Klant tijdens de Abonnementsperiode door IBM is ingelicht dat de IBM SaaS beschikbaar is, wordt er technische ondersteuning verleend via online forums en in de vorm van standaardondersteuning tijdens de periode waarin Klant verschuldigde bedragen in het kader van Betaling per Gebruik opbouwt.

Vanuit IBM SaaS kan Klant een ondersteuningsticket indienen of een chatsessie openen voor assistentie. IBM zal het IBM Software as a Service Support Handbook ter beschikking stellen, met daarin contactgegevens voor technische ondersteuning en andere informatie en processen.

Severity	Definitie van severity	Doelstellingen inzake responstijd	Dekkingsuren voor responstijd
1	**Kritieke impact op bedrijfsvoering / service down:** Bepaalde bedrijfskritische functionaliteit of een cruciale interface werkt niet. Dit heeft gewoonlijk betrekking op een productieomgeving en geeft aan dat het onmogelijk is toegang te krijgen tot de service, hetgeen kritieke gevolgen heeft voor de bedrijfsvoering. In deze situatie is onmiddellijk een oplossing vereist.	Binnen 1 uur	24x7
2	**Aanzienlijke impact op bedrijfsvoering:** Het gebruik van een bedrijfsfunctie of -voorziening van de service is ernstig beperkingt of u loopt het risico zakelijke deadlines te missen.	Binnen 2 kantooruren	Kantooruren, van maandag t/m vrijdag
3	**Kleinere impact op bedrijfsvoering:** Geeft aan dat de service of functie bruikbaar is en dat de impact op de bedrijfsvoering niet kritiek is.	Binnen vier kantooruren	Kantooruren, van maandag t/m vrijdag
4	**Minimale impact op bedrijfsvoering:** Een verzoek om informatie of een niet-technisch verzoek	Binnen 1 werkdag	Kantooruren, van maandag t/m vrijdag

4.1 Toegang tot gegevens van Klant

IBM is in staat zich toegang tot gegevens van Klant te verschaffen ten behoeve van het stellen van een diagnose bij problemen met de service, en het faciliteren van scans van de applicatie van Klant door de service. IBM zal zich uitsluitend toegang tot de gegevens verschaffen ten behoeve van het verhelpen van defecten of het verlenen van ondersteuning voor IBM-producten of -services.

5. Aanvullende bepalingen voor IBM SaaS-aanbiedingen

Bij beveiligingsscans komen mogelijkerwijs niet alle beveiligingsrisico's in een applicatie aan het licht.

De IBM SaaS kan worden gebruikt om Klant te helpen voldoen aan zijn verplichtingen inzake naleving van wet- en regelgeving (compliance), welke verplichtingen gebaseerd kunnen zijn op wetten, regelingen, normen of werkwijzen. Aanwijzingen, gebruiksadviezen of richtlijnen die door de Service worden verstrekt, vormen geen wettig, boekhoudkundig of professioneel advies en Klant wordt nadrukkelijk geadviseerd zelf deskundig advies in te winnen, juridisch of anderszins. Klant is als enige verantwoordelijk te garanderen dat Klant en de activiteiten, toepassingen en systemen van Klant voldoen aan de toepasselijke wetten, regelingen, normen en werkwijzen. Het gebruik van deze Service vormt geen garantie voor de naleving van enige wet, regeling, norm of werkwijze.

De IBM SaaS voert binnendringende en niet-binnendringende tests uit op de website en de web- of mobiele applicatie die Klant wil laten scannen. Dergelijke tests brengen bepaalde risico's met zich mee, met inbegrip van, maar niet beperkt tot de volgende:

a. de computersystemen van Klant kunnen tijdens het uitvoeren van applicaties onder de test "vastlopen", hetgeen kan leiden tot gegevensverlies of het tijdelijk niet beschikbaar zijn van de systemen;

b. de prestaties en doorvoer van de systemen van Klant, evenals de prestaties en doorvoer van bijbehorende routers en firewalls, kunnen tijdens de test tijdelijk verslechteren;

c. er kunnen buitensporige hoeveelheden logberichten worden gegenereerd, die uitzonderlijk veel schijfruimte innemen;

d. als gevolg van het onderzoeken van kwetsbaarheden kunnen er gegevens worden gewijzigd of gewist;

e. er kunnen door het inbraakdetectiesysteem alarms worden geactiveerd;

f. de verzending van e-mails kan worden gestart door de e-mailfunctie van de webapplicatie die wordt getest;

en

g. de cloudservice kan het verkeer van het bewaakte netwerk onderscheppen ten behoeve van de opsporing van events.

In geval Klant geverifieerde legitimatiegegevens voor aanmelding ("log-in") invoert voor de applicatie die onder de Service wordt getest, dient Klant uitsluitend legitimatiegegevens voor testaccounts in te voeren, niet voor productiegebruikers. Het gebruik van legitimatiegegevens van productiegebruikers kan ertoe leiden dat er via de Service persoonsgegevens worden verzonden.

De IBM SaaS kan worden geconfigureerd voor het scannen van productie-webapplicaties. Indien Klant het scantype instelt op "productie", voert de service volgens ontwerp scans uit op een wijze waarop de onderstaande risico's worden beperkt; in bepaalde situaties kan de Cloud Service echter leiden tot achteruitgang van de performance of instabiliteit binnen de geteste productiesites en -infrastructuur. IBM geeft geen enkele garantie en doet geen enkele uitspraak met betrekking tot de geschiktheid van de Cloud Service voor het scannen van productiesites.

HET IS DE VERANTWOORDELIJKHEID VAN KLANT TE BEPALEN OF DE SERVICE GESCHIKT EN VEILIG IS VOOR DE WEBSITE, WEBAPPLICATIE, MOBIELE APPLICATIE OF TECHNISCHE OMGEVING VAN KLANT.

De IBM SaaS is bedoeld voor het opsporen van een veelheid aan potentiële beveiligings- en complianceproblemen in mobiele en webapplicaties en in webservices. De Cloud Service onderzoekt niet alle kwetsbaarheden of compliancerisico's, en fungeert evenmin als barrière tegen aanvallen op de beveiliging. Beveiligingsrisico's, -regelingen en -standaarden veranderen voortdurend, en wellicht komen niet al dergelijke veranderingen tot uitdrukking in de Service. Klant is als enige verantwoordelijk voor de beveiliging en compliance van de webapplicaties, systemen en werknemers van Klant en voor eventuele herstelmaatregelen. Het is geheel aan Klant om te bepalen of de door de Service geleverde informatie al dan niet wordt gebruikt.

Pogingen computersystemen binnen te dringen of zich er toegang toe te verschaffen zijn bij wet verboden. KLANT GARANDEERT DAT HIJ DE SERVICE NIET GEBRUIKT VOOR HET SCANNEN VAN ENIGE WEBSITE EN/OF APPLICATIE ANDERS DAN DE WEBSITES EN/OF APPLICATIES DIE EIGENDOM ZIJN VAN KLANT OF DE WEBSITES EN/OF APPLICATIES WAARVOOR KLANT HET RECHT EN DE BEVOEGDHEID HEEFT ZE TE SCANNEN.

5.1 Cookies

Klant is zich ervan bewust en gaat ermee akkoord dat IBM, in het kader van de normale exploitatie en ondersteuning van de IBM SaaS, met behulp van tracerings- en andere technologie persoonsgegevens van Klant (uw werknemers en contractanten) kan verzamelen, verband houdend met het gebruik van de IBM SaaS. IBM doet dit ten behoeve van het verzamelen van gebruikscijfers en informatie over de effectiviteit van onze IBM SaaS, gericht op het verbeteren van de gebruikerservaring en/of het op maat toesnijden van interacties met Klant. Klant bevestigt toestemming te zullen verkrijgen of te hebben verkregen om IBM in staat te stellen de verzamelde persoonsgegevens, overeenkomstig de toepasselijke wetgeving, te verwerken voor de bovengenoemde doeleinden binnen IBM, andere IBM ondernemingen en hun subcontractanten, overal waar IBM en haar subcontractanten zakendoen. IBM zal voldoen aan verzoeken van werknemers en contractanten van Klant om de over hun verzamelde persoonsgegevens in te zien, bij te werken, te corrigeren en/of te wissen.

5.2 Profijt genietende locaties

Waar van toepassing worden de belastingen gebaseerd op de locatie(s) waarvan Klant aangeeft dat deze profijt geniet(en) van de IBM SaaS. Tenzij Klant IBM aanvullende informatie verstrekt, berekent IBM de belastingen op basis van het bedrijfsadres zoals dat bij het bestellen van een IBM SaaS bij IBM bekend is. Klant is verantwoordelijk voor het actueel houden van de desbetreffende informatie en voor het doorgeven van wijzigingen aan IBM.

Bijlage A

1. IBM Application Security on Cloud - Algemene beschrijving

Met IBM Application Security on Cloud heeft Klant de assistentie voor het opsporen van kwestbaarheden in de beveiliging (zoals SQL Injection, Cross-Site Scripting en Data Leakage) voor een veelheid aan applicaties op één plaats. De service omvat verschillende soorten scantechnieken voor applicatiebeveiliging, die elk de beveiligingsproblemen in de desbetreffende applicatie aangeven.

IBM Application Security on Cloud biedt de volgende mogelijkheden:

- Scanning van Mobiele Applicaties op kwetsbaarheden in de beveiliging. Dit gebeurt via dynamische (blackbox) en Interactieve (glassbox) technieken voor beveiligingsanalyse.
- Scanning van productie- of preproductiewebsites op kwetsbaarheden in de beveiliging. Dit gebeurt via dynamische (blackbox) technieken voor beveiligingsanalyse.
- Scanning van de gegevensstromen binnen web- en desktopapplicaties op kwetsbaarheden in de beveiliging. Dit gebeurt via statische (whitebox) technieken voor beveiligingsanalyse.
- Gedetailleerde rapporten inzake kwetsbaarheden in de beveiliging, met zowel overkoepelende overzichten van de bevindingen als verbeteringsprocedures die door ontwikkelaars kunnen worden gevolgd.
- Integratie met diverse DevOps-platforms zoals Maven en IBM UrbanCode