

## Termenii de Utilizare IBM – Termeni Specifici Ofertei SaaS

### IBM Application Security on Cloud

Termenii de Utilizare ("TdU") sunt alcătuiți din acești Termeni de Utilizare IBM – Termeni Specifici Ofertei SaaS ("Termenii Specifici Ofertei SaaS") și un document intitulat Termenii de Utilizare IBM – Termeni Generali ("Termenii Generali"), disponibil la următorul URL: <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

În eventualitatea unui conflict, Termenii Specifici Ofertei SaaS vor prevala față de Termenii Generali. Prin comandarea, accesarea sau utilizarea IBM SaaS, Clientul este de acord cu Termenii de Utilizare.

Termenii de Utilizare sunt guvernați de IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement sau IBM International Agreement for Selected IBM SaaS Offerings, după caz ("Contractul"), care împreună cu Termenii de Utilizare reprezintă acordul complet.

#### 1. IBM SaaS

Acești Termeni Specifici Ofertei SaaS acoperă următoarele oferte IBM SaaS:

- IBM Application Security Analyzer

#### 2. Indicii de Măsurare pentru Tarifare

IBM SaaS este vândut în baza următorilor indici de măsurare pentru tarifare, după cum este specificat în Documentul Tranzacțional:

- Instanță de Aplicație** – este o unitate de măsură pentru obținerea IBM SaaS. Este necesar câte un drept Instanță de Aplicație pentru fiecare instanță a unei Aplicații conectate la IBM SaaS. Dacă o Aplicație are mai multe componente, fiecare servind un scop distinct și/sau o bază de utilizator și fiecare fiind conectată la sau gestionată de IBM SaaS, atunci fiecare dintre aceste componente este considerată o Aplicație separată. În plus, mediile de testare, dezvoltare, intermediere și producție pentru o Aplicație sunt considerate, fiecare, câte o instanță separată a Aplicației și pentru fiecare este necesar un drept de utilizare. Când există mai multe instanțe ale Aplicației într-un singur mediu, fiecare este considerată o instanță separată a Aplicației și fiecare necesită un drept de utilizare. Trebuie obținute drepturi suficiente pentru a acoperi numărul Instanțelor de Aplicație conectate la IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacțional al Clientului.
- Acces** – este o unitate de măsură pentru obținerea IBM SaaS. Un Acces înseamnă dreptul de a utiliza IBM SaaS. Clientul trebuie să obțină un singur drept Acces în vederea utilizării IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (PoE) sau Documentul Tranzacțional al Clientului.

#### 3. Tarife și Facturare

Suma de plată pentru IBM SaaS este specificată într-un Document Tranzacțional.

##### 3.1 Plată per Utilizare

Opțiunile Plată per Utilizare vor fi facturate în luna următoare utilizării serviciului, la rata specificată în Documentul Tranzacțional.

##### 3.2 Tarif Lunar Parțial

Un tarif lunar parțial, după cum este specificat în Documentul Tranzacțional, poate fi evaluat prin proratare.

#### 4. Suport Tehnic

Pe durata Perioadei de Abonare, după ce IBM anunță Clientul că este disponibil accesul la IBM SaaS, este furnizat suport tehnic prin forumuri online și ca suport standard pe durata perioadei în care Clientul ocazional plătește tarife Plată per Utilizare. Din IBM SaaS, Clienții pot să trimită un tichet de suport sau să deschidă o sesiune de chat pentru asistență. IBM va face disponibilă publicația IBM Software as a Service Support Handbook, care conține informații privind contactarea suportului tehnic și alte informații și procese.

Severitate	Definiție Severitate	Obiective Timp de Răspuns	Acoperire Timp de Răspuns
1	<b>Impact critic asupra afacerii/serviciu întrerupt:</b> O funcționalitate cu caracter critic pentru afacere este inoperabilă sau nu funcționează o interfață cu caracter critic. De obicei aceasta se aplică în cazul unui mediu de producție și indică incapacitatea de a accesa serviciile, ceea ce are un impact critic asupra operațiilor. Această condiție necesită o soluționare imediată.	Într-un interval de 1 oră	24x7
2	<b>Impact semnificativ asupra afacerii:</b> O caracteristică sau o funcție a serviciului a suferit o restricție importantă și riscați să nu puteți îndeplini termenele limită ale afacerii.	Într-un interval de 2 ore de lucru	Orele de lucru L-V
3	<b>Impact minor asupra afacerii:</b> Indică situația în care serviciul sau funcționalitatea permite utilizarea și nu are un impact critic asupra operațiilor.	Într-un interval de 4 ore de lucru	Orele de lucru L-V
4	<b>Impact minim asupra afacerii:</b> O întrebare sau o cerere care nu are caracter tehnic	Într-un interval de 1 zi lucrătoare	Orele de lucru L-V

#### 4.1 Accesul la Datele Clientului

IBM va putea să acceseze datele Clientului, în vederea diagnosticării problemelor legate de serviciu și pentru facilitarea scanărilor aplicației Clientului de către serviciu. IBM va accesa datele numai în scopul remedierii defectelor sau pentru a furniza suport pentru produsele sau serviciile IBM.

#### 5. Termeni Suplimentari pentru Oferta IBM SaaS

Este posibil ca Scanările de Securitate să nu identifice toate riscurile de securitate într-o aplicație.

IBM SaaS poate fi utilizat pentru a ajuta Clientul să își îndeplinească obligațiile privind conformitatea, care pot fi bazate pe legi, reglementări, standarde sau practici. Indicațiile, sugestiile de utilizare sau ghidările furnizate de Serviciu nu reprezintă o îndrumare legală, de contabilitate sau alt tip de sfat profesional, iar Clientul este sfătuit să apeleze la propria consiliere legală sau la altă astfel de consiliere expertă. Clientul este singurul responsabil pentru asigurarea faptului că Clientul, activitățile, aplicațiile și sistemele lui se conformează tuturor legilor, reglementărilor, standardelor și practicilor în vigoare. Utilizarea acestui Serviciu nu garantează conformitatea cu legile, reglementările, standardele sau practicile.

IBM SaaS realizează testări invazive și neinvazive pentru website-ul și aplicația web sau mobilă pe care Client le alege pentru scanare, testarea fiind însoțită de anumite riscuri, incluzând, dar fără a se limita la, următoarele:

- în timpul rulării aplicațiilor incluse în testare, este posibil ca sistemele informatice ale Clientului să se blocheze sau să nu mai funcționeze corespunzător, având ca rezultat indisponibilitatea temporară a sistemelor sau pierderea de date;
- nivelurile de performanță și transfer ale sistemelor Clientului, precum și ale router-elor și firewall-urilor asociate, pot suferi o degradare temporară în timpul testării;
- poate fi generat un volum excesiv de mesaje de istoric, determinând un consum exagerat al spațiului de disc alocat fișierului istoric;
- este posibil să fie modificate sau șterse date ca urmare a vulnerabilităților testate;
- pot fi declanșate alarme de către sistemele de detectare a intruziunii;
- pot fi trimise e-mail-uri prin declanșarea funcției de e-mail a aplicației web testate;
- și
- serviciul cloud poate intercepta traficul rețelei monitorizate, în vederea căutării evenimentelor.

În eventualitatea în care Clientul introduce acreditări de logare autentificate pentru aplicația testată în cadrul Serviciului, Clientul ar trebui să introducă astfel de acreditări numai pentru conturile de testare, nu și pentru utilizatorii de producție. Utilizarea acreditărilor de utilizator de producție poate determina transmiterea datelor personale prin intermediul Serviciului.

Se poate configura IBM SaaS pentru scanarea aplicațiilor web de producție. Atunci când Clientul setează tipul de scanare la "producție", serviciul este proiectat să realizeze scanările astfel încât să fie diminuate riscurile prezentate mai sus; totuși, în anumite situații, Serviciul Cloud poate determina degradarea performanței sau instabilitatea site-urilor și infrastructurii de producție testate. IBM nu oferă nicio garanție sau declarație privind gradul de adecvare al utilizării Serviciului Cloud pentru scanarea site-urilor de producție.

**ESTE RESPONSABILITATEA CLIENTULUI DE A DETERMINA DACĂ SERVICIUL ESTE CORESPUNZĂTOR SAU SIGUR PENTRU WEBSITE-UL, APLICAȚIA WEB, APLICAȚIA MOBILĂ SAU MEDIUL TEHNIC AL CLIENTULUI.**

IBM SaaS este conceput pentru a identifica o gamă largă de probleme posibile privind securitatea și conformitatea aplicațiilor mobile și web și a serviciilor web. El nu testează toate vulnerabilitățile sau riscurile legate de conformitate și nici nu acționează ca o barieră în calea atacurilor privind securitatea. Amenințările privind securitatea, reglementările și standardele se modifică încontinuu, iar Serviciul nu poate reflecta toate aceste modificări. Securitatea și conformitatea aplicațiilor web, sistemelor și angajaților Clientului, precum și orice acțiuni de remediere, reprezintă responsabilitatea exclusivă a Clientului. Ține exclusiv de decizia Clientului dacă vor fi utilizate sau nu informațiile furnizate de către Serviciu.

Anumite legi interzic orice încercare neautorizată de a penetra sau accesa sistemele informatice. **ESTE RESPONSABILITATEA CLIENTULUI DE A SE ASIGURA CĂ NU UTILIZEAZĂ SERVICIUL PENTRU SCANAREA ALTOR WEBSITE-URI ȘI/SAU APLICAȚII ÎN AFARA WEBSITE-URILOR ȘI/SAU APLICAȚIILOR DEȚINUTE DE CLIENT SAU PENTRU CARE CLIENTUL ARE DREPTUL ȘI AUTORITATEA PENTRU SCANARE.**

## **5.2 Cookie-uri**

Clientul este conștient și acceptă că IBM poate, ca parte a operării normale și asigurării suportului pentru IBM SaaS, să colecteze informații personale de la Client (angajații și contractorii dumneavoastră) privind utilizarea IBM SaaS, prin urmărire și alte tehnologii. IBM face aceasta pentru a colecta statistici privind utilizarea și informații despre eficiența IBM SaaS, în vederea îmbunătățirii experienței de utilizator și/sau pentru ajustarea interacțiunilor cu Clientul. Clientul confirmă că va obține sau va avea consimțământul pentru a permite ca IBM să proceseze informațiile personale colectate pentru scopul menționat mai sus, în cadrul IBM, în alte companii IBM și în cele ale subcontractorilor săi, în care noi sau subcontractorii noștri ne desfășurăm activitatea, în conformitate cu legile aplicabile. IBM se va conforma solicitărilor angajaților și contractorilor Clientului privind accesarea, actualizarea, corectarea sau ștergerea informațiilor lor personale colectate.

## **5.3 Locații de Beneficiu Derivate**

Când este aplicabil, taxele sunt bazate pe locațiile pe care Clientul le identifică ca loc unde beneficiază de IBM SaaS. IBM va aplica taxele utilizând adresa de afaceri specificată ca locație principală de beneficiu, atunci când se comandă un IBM SaaS, cu excepția cazului în care IBM primește alte informații de la Client. Clientul este responsabil pentru păstrarea acestor informații și trimiterea oricărei modificări la IBM.

## Anexa A

### 1. IBM Application Security on Cloud - Descriere Generală

IBM Application Security on Cloud asigură un loc central pentru asistarea Clientului la identificarea vulnerabilităților de securitate (SQL Injection, Cross-Site Scripting și Data Leakage) pentru diverse aplicații. Serviciul include diverse tipuri de scanare a aplicațiilor, pentru identificarea problemelor de securitate ale aplicației respective.

IBM Application Security on Cloud furnizează următoarele capabilități:

- Scanarea aplicațiilor mobile, pentru depistarea vulnerabilităților de securitate. Aceasta este realizată pe baza unor tehnologii de analiză a securității dinamice (blackbox) și interactive (glassbox).
- Scanarea site-urilor Web de producție sau pre-producție, pentru depistarea vulnerabilităților de securitate. Aceasta este realizată pe baza unor tehnici de analiză a securității dinamice (blackbox).
- Scanarea fluxurilor de date din aplicațiile Web și Desktop, pentru depistarea vulnerabilităților de securitate. Aceasta este realizată pe baza unor tehnici de analiză a securității statice (whitebox).
- Rapoarte detaliate privind vulnerabilitățile de securitate, care includ atât sumare de nivel înalt ale rezultatelor, cât și pașii pe care dezvoltatorii îi pot parcurge pentru remediere.
- Integrarea cu diverse platforme DevOps, cum ar fi Maven și IBM UrbanCode