IBM Application Security on Cloud

Syarat-syarat Penggunaan ("ToU") terdiri dari Syarat-syarat Penggunaan IBM – Syarat-syarat Tawaran Spesifik SaaS ("Syarat-syarat Tawaran Spesifik SaaS") ini dan sebuah dokumen berjudul Syarat-syarat Penggunaan IBM – Syarat-syarat Umum ("Syarat-syarat Umum") yang tersedia di URL berikut: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Apabila terdapat ketidaksesuaian, Syarat-syarat Tawaran Spesifik SaaS akan berlaku di atas Syarat-syarat Umum. Dengan memesan, mengakses, atau menggunakan SaaS IBM, Klien menyetujui ToU.

ToU diatur oleh Perjanjian Keuntungan Paspor Internasional IBM, Perjanjian Ekspres Keuntungan Paspor Internasional IBM, atau Perjanjian Internasional IBM untuk Tawaran SaaS IBM Terpilih, sebagaimana yang berlaku ("Perjanjian") dan bersama dengan ToU merupakan perjanjian yang lengkap.

1. SaaS IBM

Tawaran SaaS IBM berikut dicakup oleh Syarat-syarat Tawaran Spesifik SaaS ini:

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

2. Metrik Biaya

SaaS IBM dijual berdasarkan metrik biaya berikut, sebagaimana yang ditetapkan dalam Dokumen Transaksi:

a. **Pekerjaan** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Pekerjaan merupakan suatu objek di dalam SaaS IBM yang tidak dapat dibagi lagi dan mewakili proses komputasi termasuk seluruh sub-prosesnya. Kepemilikan yang memadai harus diperoleh untuk mencakup total jumlah Pekerjaan yang diproses atau dikelola oleh SaaS IBM selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

b. **Mesin Virtual Aplikasi** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Kepemilikan atas suatu Mesin Virtual Aplikasi diperlukan untuk setiap mesin virtual dari suatu Aplikasi yang terhubung ke SaaS IBM. Apabila suatu Aplikasi memiliki beberapa komponen, yang masing-masing memiliki tujuan dan/atau dasar pengguna yang berbeda, dan masing-masing komponen darinya dapat dihubungkan ke atau dikelola oleh SaaS IBM, masing-masing komponen tersebut dianggap sebagai Aplikasi yang terpisah. Selain itu, lingkungan pengujian, pengembangan, *staging*, dan produksi untuk suatu Aplikasi masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi dan masing-masing harus mempunyai kepemilikan. Beberapa Mesin Virtual Aplikasi dalam suatu lingkungan tunggal masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi tersebut dan masing-masing harus mempunyai kepemilikan. Kepemilikan yang memadai harus diperoleh untuk mencakup jumlah Mesin Virtual Aplikasi yang terhubung ke SaaS IBM selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

c. **Mesin Virtual** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Suatu Mesin Virtual adalah akses ke suatu konfigurasi spesifik dari SaaS IBM. Kepemilikan yang memadai harus diperoleh untuk setiap Mesin Virtual (*Instance*) SaaS IBM yang tersedia untuk akses dan penggunaan selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

   Untuk setiap kepemilikan Mesin Virtual, tidak ada batas untuk jumlah Pekerjaan yang dilakukan atau Mesin Virtual Aplikasi (Aplikasi yang terhubung), dengan ketentuan bahwa, tidak lebih dari 30 Pekerjaan dapat dijalankan pada suatu waktu tertentu.

3. Biaya dan Penagihan

Jumlah yang harus dibayarkan untuk SaaS IBM ditetapkan dalam Dokumen Transaksi.

3.1 Bayar per Penggunaan (*Pay per Use*)

Opsi Bayar per Penggunaan akan ditagih pada bulan setelah bulan ketika layanan digunakan pada tarif yang ditetapkan dalam Dokumen Transaksi.

3.2 Biaya Pertengahan Bulan (*Partial Month Charge*)

Biaya pertengahan bulan sebagaimana yang ditetapkan dalam Dokumen Transaksi dapat dinilai secara pro-rata.

4. Jangka Waktu dan Opsi Pembaruan

Jangka waktu SaaS IBM dimulai pada tanggal ketika IBM memberi tahu Klien mengenai akses mereka ke SaaS IBM, sebagaimana yang didokumentasikan dalam PoE. PoE akan menetapkan apakah SaaS IBM memperbarui secara otomatis, berlanjut berdasarkan penggunaan berkelanjutan, atau berakhir pada akhir jangka waktu.

Untuk pembaruan otomatis, kecuali apabila Klien memberikan pemberitahuan tertulis untuk tidak memperbarui setidaknya 90 hari sebelum tanggal habis masa berlakunya jangka waktu, SaaS IBM akan secara otomatis memperbarui untuk jangka waktu yang ditetapkan dalam PoE.

Untuk penggunaan berkelanjutan, SaaS IBM akan terus tersedia dengan basis per bulan hingga Klien memberikan pemberitahuan tertulis 90 hari sebelumnya mengenai pengakhiran. SaaS IBM akan tetap tersedia hingga akhir bulan kalender setelah periode 90 hari tersebut.

5. Dukungan Teknis

Selama Periode Langganan dan setelah IBM memberi tahu Klien bahwa akses ke Saas IBM tersedia, dukungan teknis diberikan melalui forum *online* dan sebagai dukungan standar selama periode waktu di mana Klien dikenai biaya Bayar per Penggunaan (*Pay per Use*). Dari dalam SaaS IBM, Klien dapat mengajukan tiket dukungan atau membuka sesi obrolan untuk mendapatkan bantuan. IBM akan menyediakan Buku Petunjuk Dukungan Perangkat Lunak sebagai Layanan IBM yang memberikan informasi kontak dukungan teknis serta informasi dan proses lain.

Tingkat Permasalahan	Definisi Tingkat Permasalahan	Sasaran Waktu Tanggapan	Cakupan Waktu Tanggapan
1	**Pengaruh bisnis penting/layanan bermasalah:** Fungsi penting bisnis tidak dapat beroperasi atau antarmuka penting telah gagal. Hal ini biasanya berlaku pada lingkungan produksi dan mengindikasikan ketidakmampuan untuk mengakses layanan yang berpengaruh penting pada pengoperasian. Kondisi ini memerlukan solusi yang mendesak.	Dalam 1 jam	24x7
2	**Pengaruh bisnis yang signifikan:** Suatu fitur bisnis layanan atau fungsi dari layanan sangat terbatas dalam penggunaannya atau Anda berisiko melewati tenggat waktu bisnis.	Dalam 2 jam kerja	Jam kerja S-J
3	**Pengaruh bisnis minor:** Mengindikasikan fungsi atau layanan dapat digunakan dan tidak berpengaruh penting terhadap pengoperasian.	Dalam 4 jam kerja	Jam kerja S-J
4	**Pengaruh bisnis minimum:** Pertanyaan atau permintaan non-teknis	Dalam 1 hari kerja	Jam kerja S-J

5.1 Akses ke Data Klien

IBM akan dapat mengakses data Klien untuk tujuan mendiagnosis masalah dengan layanan, dan mempermudah pemindaian aplikasi Anda oleh layanan. IBM akan mengakses data hanya untuk tujuan memperbaiki kecacatan atau menyediakan dukungan untuk layanan atau produk IBM.

6. Syarat-syarat Tambahan Tawaran SaaS IBM

Pemindaian keamanan mungkin tidak dapat mengidentifikasi semua risiko keamanan dalam suatu aplikasi.

SaaS IBM dapat digunakan untuk membantu Klien memenuhi kewajiban kepatuhan, yang dapat didasarkan pada peraturan perundang-undangan, regulasi, standar atau kebiasaan umum. Setiap petunjuk, anjuran penggunaan atau panduan yang diberikan oleh Layanan bukan merupakan nasihat hukum, akuntansi atau nasihat profesional lainnya, dan Klien diperingatkan untuk mendapatkan nasihat ahli hukum atau ahli lainnya sendiri. Klien sepenuhnya bertanggung jawab untuk memastikan bahwa Klien serta aktivitas, aplikasi, dan sistem Klien mematuhi seluruh peraturan perundang-undangan, regulasi, standar, dan kebiasaan umum yang berlaku. Penggunaan Layanan ini tidak menjamin kepatuhan terhadap setiap peraturan perundang-undangan, regulasi, standar atau kebiasaan umum.

SaaS IBM melakukan pengujian invasif dan non-invasif pada situs web dan aplikasi *mobile* atau web yang dipilih oleh Klien untuk dipindai, di mana pengujian tersebut memiliki risiko tertentu, termasuk namun tidak terbatas pada hal berikut:

a. sistem komputer Klien saat menjalankan aplikasi yang diuji dapat terhenti atau terganggu, yang mengakibatkan sistem tidak tersedia untuk sementara atau hilangnya data;

b. kinerja dan *throughput* sistem Klien, serta kinerja dan *throughput* dari *router* dan *firewall* terkait, dapat diturunkan sementara selama pengujian;

c. jumlah pesan catatan (*log messages*) yang berlebihan dapat dihasilkan, yang mengakibatkan penggunaan ruang disk file catatan (*log file*) menjadi berlebih;

d. data dapat diubah atau dihapus sebagai akibat dari pemeriksaan terhadap kerentanan;

e. alarm dapat terpicu oleh sistem deteksi intrusi;

f. email dapat terpicu oleh fungsi email dari aplikasi web yang sedang diuji;

g. SaaS IBM dapat menghalangi lalu lintas jaringan yang dipantau untuk tujuan mencari peristiwa.

Apabila Klien memasukkan kredensial log-in yang telah diotentikasi untuk aplikasi yang diuji ke dalam Layanan, Klien harus memasukkan kredensial tersebut hanya untuk akun pengujian dan bukan untuk pengguna produksi. Penggunaan kredensial pengguna produksi dapat mengakibatkan data pribadi ditransmisikan melalui Layanan.

SaaS IBM dapat dikonfigurasikan untuk memindai aplikasi web produksi. Saat Klien menetapkan jenis pemindaian sebagai "produksi", layanan dirancang untuk menjalankan pemindaian dengan cara yang mengurangi risiko-risiko yang tercantum di atas; namun, dalam situasi tertentu, SaaS IBM dapat mengakibatkan penurunan kinerja atau ketidakstabilan dalam infrastruktur dan situs-situs produksi yang diuji. IBM tidak membuat jaminan atau pernyataan apa pun sehubungan dengan kesesuaian penggunaan SaaS IBM untuk memindai situs produksi.

KLIEN BERTANGGUNG JAWAB UNTUK MENENTUKAN APAKAH LAYANAN TELAH SESUAI ATAU AMAN UNTUK SITUS WEB, APLIKASI WEB, APLIKASI MOBILE, ATAU LINGKUNGAN TEKNIS KLIEN.

SaaS IBM dirancang untuk mengidentifikasi berbagai potensi masalah keamanan dan kepatuhan dalam aplikasi web dan *mobile* serta layanan web. Layanan ini tidak menguji semua risiko kerentanan atau kepatuhan, juga tidak bertindak sebagai penghalang terhadap serangan keamanan. Ancaman keamanan, regulasi, dan standar terus-menerus berubah, dan Layanan mungkin tidak merefleksikan semua perubahan tersebut. Keamanan dan kepatuhan aplikasi web, sistem dan karyawan Klien, serta tindakan perbaikan apa pun, merupakan tanggung jawab Klien sepenuhnya. Atas kebijakannya sendiri Klien dapat memilih untuk menggunakan atau tidak menggunakan informasi apa pun yang disediakan oleh Layanan.

Peraturan perundang-undangan tertentu melarang setiap upaya yang tidak sah untuk memasuki atau mengakses sistem komputer. KLIEN BERTANGGUNG JAWAB UNTUK MEMASTIKAN BAHWA KLIEN TIDAK MENGGUNAKAN LAYANAN UNTUK MEMINDAI SITUS WEB DAN/ATAU APLIKASI APA PUN SELAIN SITUS WEB DAN/ATAU APLIKASI YANG DIMILIKI OLEH KLIEN ATAU YANG UNTUKNYA KLIEN MEMILIKI HAK DAN OTORITAS UNTUK MEMINDAI.

6.2 Cookies

Klien menyadari dan menyetujui bahwa IBM dapat, sebagai bagian dari dukungan dan operasi normal atas SaaS IBM, mengumpulkan informasi pribadi dari Klien (kontraktor dan karyawan Anda) terkait dengan penggunaan SaaS IBM, melalui pelacakan dan teknologi lainnya. IBM melakukan hal tersebut

untuk mengumpulkan informasi dan statistik penggunaan mengenai keefektifan dari SaaS IBM kami untuk tujuan meningkatkan pengalaman pengguna dan/atau menyesuaikan interaksi dengan Klien. Klien mengonfirmasikan bahwa pihaknya akan atau telah memperoleh persetujuan untuk mengizinkan IBM memproses informasi pribadi yang dikumpulkan untuk tujuan di atas dalam IBM, perusahaan(-perusahaan) IBM lainnya dan subkontraktor mereka, di mana pun kami dan subkontraktor kami melakukan bisnis, sesuai dengan hukum yang berlaku. IBM akan mematuhi permintaan dari kontraktor dan karyawan Klien untuk mengakses, memperbarui, memperbaiki atau menghapus informasi pribadi mereka yang dikumpulkan.

6.3 Lokasi Manfaat yang Diperoleh

Apabila berlaku, pajak akan didasarkan pada lokasi(-lokasi) yang diidentifikasi oleh Klien sebagai penerima manfaat dari SaaS IBM. IBM akan menerapkan pajak berdasarkan alamat bisnis yang dicantumkan pada saat memesan SaaS IBM sebagai lokasi manfaat utama kecuali apabila Klien memberikan informasi tambahan kepada IBM. Klien bertanggung jawab untuk tetap memperbarui informasi tersebut dan menyampaikan setiap perubahan kepada IBM.

Apendiks A

1. Deskripsi Umum IBM Application Security on Cloud

IBM Application Security on Cloud memberikan suatu tempat tunggal untuk membantu Klien dalam mengidentifikasi kerentanan keamanan (seperti Injeksi SQL, *Scripting* Lintas Situs (*Cross-Site Scripting*), dan Kebocoran Data) untuk berbagai aplikasi. Layanan mencakup berbagai jenis teknik pemindaian keamanan aplikasi, yang masing-masing mengidentifikasi masalah keamanan dalam aplikasi tersebut.

IBM Application Security on Cloud memberikan kemampuan berikut:

- Memindai Aplikasi Mobile untuk kerentanan keamanan. Hal ini dilakukan melalui teknologi analisis keamanan dinamis (*blackbox*) dan Interaktif (*glassbox*).
- Memindai situs Web produksi atau pra-produksi di jaringan publik atau pribadi, untuk kerentanan keamanan. Hal ini dilakukan melalui teknik analisis keamanan dinamis (*blackbox*).
- Memindai aliran data dalam aplikasi Web dan Desktop untuk kerentanan keamanan. Hal ini dilakukan melalui teknik analisis keamanan statis (*whitebox*).
- Laporan kerentanan keamanan terperinci yang mencakup ringkasan tingkat tinggi tentang temuan dan langkah-langkah perbaikan yang dapat dilakukan oleh pengembang.
- Integrasi dengan berbagai platform DevOps

This Agreement is made in the English and Indonesian languages. To the extent permitted by the prevailing law, the English language of this Agreement will prevail in the case of any inconsistencies or differences of interpretation with the Indonesian language text of this Agreement.
Perjanjian ini dibuat dalam Bahasa Indonesia dan Bahasa Inggris. Sepanjang diperbolehkan oleh hukum yang berlaku, dalam hal terdapat ketidaksesuaian atau perbedaan penafsiran dengan teks Bahasa Indonesia dari Perjanjian ini, maka teks dalam Bahasa Inggris yang akan berlaku