

Syarat-syarat Penggunaan IBM – Syarat-syarat Tawaran Spesifik SaaS

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 Syarat-syarat Penggunaan.

Syarat-syarat Penggunaan 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 Syarat-syarat Penggunaan merupakan perjanjian yang lengkap.

1. SaaS IBM

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

- Penganalisis Keamanan IBM

2. Metrik Biaya

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

- Mesin Virtual Aplikasi** – adalah unit ukuran yang olehnya SaaS IBM dapat diperoleh. Suatu kepemilikan atas Mesin Virtual Aplikasi diperlukan untuk setiap mesin virtual dari Aplikasi yang terhubung ke SaaS IBM. Apabila Aplikasi memiliki banyak komponen, masing-masing menjalankan tujuan yang berbeda dan/atau dasar pengguna, dan masing-masing aplikasi dapat dihubungkan ke atau dikelola oleh SaaS IBM, masing-masing komponen tersebut dianggap sebagai Aplikasi yang terpisah. Selain itu, lingkungan pengujian, pengembangan, penahapan, dan produksi untuk suatu Aplikasi masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi dan masing-masing harus memiliki kepemilikan. Sejumlah mesin virtual Aplikasi dalam suatu lingkungan tunggal masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi dan masing-masing harus memiliki 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.
- Akses** – adalah unit ukuran yang olehnya SaaS IBM dapat diperoleh. Akses adalah hak untuk menggunakan SaaS IBM. Klien harus memperoleh kepemilikan Akses tunggal untuk menggunakan SaaS IBM selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

3. Biaya dan Penagihan

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

3.1 Pay as you Go

Opsi Pay as you Go akan ditagihkan pada bulan berikutnya ketika layanan digunakan pada tarif yang ditetapkan dalam Dokumen Transaksi.

3.2 Biaya Pertengahan Bulan (*Partial Month Charges*)

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

4. Dukungan Teknis

Selama Periode Langganan dan setelah IBM memberitahukan kepada Klien bahwa akses ke SaaS IBM tersedia, dukungan teknis diberikan melalui forum online dan sebagai dukungan Standar selama periode waktu yang mana klien dikenai biaya Pay as You Go. Dari dalam SaaS IBM, klien dapat mengirimkan tiket dukungan atau membuka sesi obrolan untuk bantuan. IBM akan menyediakan Buku Panduan

Dukungan Perangkat Lunak sebagai Layanan IBM yang memberikan informasi kontak dukungan teknis dan informasi serta 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 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 layanan menjadi sangat terbatas penggunaannya atau Anda berisiko melewatkan 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 minimal: Pertanyaan atau permintaan non-teknis | Dalam 1 hari kerja | Jam kerja S-J |

4.1 Akses ke Data Klien

IBM akan dapat untuk mengakses data Klien untuk tujuan mendiagnosis masalah yang terjadi dengan layanan, dan akan memfasilitasi pemindaian aplikasi Anda oleh layanan. IBM akan mengakses data hanya untuk tujuan memperbaiki kerusakan atau memberikan dukungan untuk layanan atau produk IBM.

5. Syarat-syarat Tambahan Tawaran SaaS IBM

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

SaaS IBM dapat digunakan untuk membantu Klien dalam memenuhi kewajiban-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 advis hukum, akuntansi atau advis profesional lainnya, dan Klien diperingatkan untuk mendapatkan advis dari penasihat hukumnya sendiri atau penasihat ahli lainnya. Klien semata-mata bertanggung jawab untuk memastikan bahwa Klien serta kegiatan, aplikasi, dan sistem Klien mematuhi semua peraturan perundang-undangan, regulasi, standar, dan kebiasaan umum yang berlaku. Penggunaan Layanan ini tidak menjamin kepatuhan terhadap setiap hukum, regulasi, standar atau kebiasaan umum.

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

- a. sistem komputer Klien saat menjalankan aplikasi pada saat pengujian berlangsung dapat menjadi terhenti sementara atau *crash*, mengakibatkan sistem tidak tersedia untuk sementara atau data hilang;
- b. kinerja dan throughput dari sistem Klien, serta kinerja dan *throughput* dari *router* dan *firewall* terkait, dapat diturunkan sementara selama pengujian;
- c. jumlah catatan pesan (*log messages*) yang terlampaui banyak dapat dihasilkan, mengakibatkan konsumsi kapasitas *disk file* catatan (*log*) menjadi berlebih;
- d. data dapat diubah atau dihapus sebagai akibat dari pemeriksaan terhadap kerentanan;
- e. alarm dapat dipicu oleh sistem deteksi intrusi;
- f. email dapat dipicu oleh fungsi *email* dari aplikasi *web* yang sedang diuji;

g. layanan cloud dapat menghalangi lalu lintas jaringan yang dipantau untuk tujuan mencari peristiwa. Dalam hal Klien memasukkan kredensial *log-in* yang telah diotentikasikan untuk aplikasi berdasarkan pengujian ke dalam Layanan, Klien hanya harus memasukkan kredensial tersebut untuk akun pengujian dan bukan untuk pengguna produksi. Penggunaan kredensial pengguna produksi dapat mengakibatkan data pribadi dikirimkan melalui Layanan.

SaaS IBM dapat dikonfigurasi untuk memindai aplikasi *web* produksi. Saat Klien menetapkan jenis pemindaian sebagai "produksi", layanan dirancang untuk menjalankan pemindaian dengan cara yang mengurangi risiko yang tercantum di atas; namun demikian, dalam situasi tertentu, Layanan Cloud dapat mengakibatkan penurunan kinerja atau ketidakstabilan di dalam situs-situs produksi dan infrastruktur yang diuji. IBM tidak membuat jaminan atau pernyataan sehubungan dengan kesesuaian menggunakan Layanan Cloud 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 layanan aplikasi *web* dan *mobile* dan layanan *web*. SaaS IBM tidak menguji semua risiko kepatuhan atau kerentanan, ataupun bertindak sebagai penghalang terhadap serangan keamanan. Ancaman keamanan, regulasi, dan standar terus berubah, dan Layanan mungkin tidak dapat merefleksikan semua perubahan tersebut. Keamanan dan kepatuhan aplikasi *web*, sistem dan karyawan Klien, serta tindakan pemulihan apa pun, merupakan tanggung jawab Klien sepenuhnya. Hal tersebut semata-mata merupakan kebijakan Klien untuk menggunakan atau tidak menggunakan informasi apa pun yang diberikan 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 PELANGGAN MEMILIKI HAK DAN OTORITAS UNTUK MEMINDAINYA.**

5.2 Cookies

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

5.3 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 tercantum 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 merangkul kemampuan untuk memeriksa aplikasi *web* dan *mobile* Android dengan cara yang sangat mudah. Layanan mengidentifikasi masalah keamanan di dalam aplikasi dan menghasilkan laporan keamanan yang mencakup langkah-langkah perbaikan yang dapat diikuti oleh pengembang.

Penganalisis Keamanan IBM ditawarkan sebagai tawaran langganan dan dengan cara membayar sesuai penggunaan. Jika Klien berhak atas tawaran pembayaran per penggunaan, kepemilikan Akses akan ditetapkan untuk Keamanan Aplikasi IBM di Cloud untuk mengaktifkan opsi pembayaran per penggunaan.

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.