IBM Security Trusteer Fraud Protection

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 ini.

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 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:

1.1 Tawaran SaaS Rapport IBM

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Rapport for Business Premium Support
- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Rapport for Retail Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Security Trusteer Rapport Mandatory Service for Business
- IBM Security Trusteer Rapport Mandatory Service for Retail

1.2 Tawaran SaaS IBM Pinpoint

- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Premium Support

- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile Premium Support
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Business
- IBM Security Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Security Trusteer Rapport Remediation for Retail
- IBM Security Trusteer Rapport Remediation for Retail Premium Support

1.3 Tawaran SaaS IBM Mobile

- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Business
- IBM Security Trusteer Mobile Browser for Business Premium Support
- IBM Security Trusteer Mobile Browser for Retail
- IBM Security Trusteer Mobile Browser for Retail Premium Support

2. Metrik Biaya

SaaS IBM dijual berdasarkan salah satu metrik(-metrik) biaya berikut sebagaimana yang ditetapkan dalam Dokumen Transaksi:

a. **Peserta yang Memenuhi Syarat** – adalah unit ukuran yang olehnya SaaS IBM dapat diperoleh. Setiap individu atau entitas yang memenuhi syarat untuk berpartisipasi dalam program penyampaian layanan apa pun yang dikelola atau dilacak dengan SaaS IBM adalah Peserta yang Memenuhi Syarat. Kepemilikan yang memadai harus diperoleh untuk mencakup seluruh Peserta yang Memenuhi Syarat yang dikelola atau dilacak dalam SaaS IBM selama periode pengukuran yang ditetapkan dalam Dokumen Transaksi Klien.

   Setiap program penyampaian layanan yang dikelola oleh SaaS IBM dianalisis secara terpisah dan kemudian ditambahkan bersama-sama. Individu atau entitas yang memenuhi syarat untuk beberapa program penyampaian layanan memerlukan kepemilikan yang terpisah.

   Untuk tawaran ini, program penyampaian layanan mencakup Aplikasi Bisnis atau Ritel tunggal Klien dengan halaman login utama dan halaman terkait untuk setiap Aplikasi Bisnis atau Ritel. Peserta yang Memenuhi Syarat adalah pengguna akhir dari Klien, yang memiliki kredensial untuk login pada Aplikasi Bisnis atau Ritel.

b. **Perangkat Klien** – adalah unit ukuran yang olehnya SaaS IBM dapat diperoleh. Perangkat Klien adalah perangkat komputasi pengguna tunggal atau sensor tujuan khusus atau perangkat telemetri yang meminta pelaksanaan atau penerimaan untuk pelaksanaan kumpulan perintah, prosedur, atau aplikasi dari atau memberikan data ke sistem komputer lain yang biasanya disebut sebagai server atau jika tidak dikelola oleh server. Beberapa Perangkat Klien dapat berbagi akses ke server yang umum. Perangkat Klien dapat memiliki beberapa kemampuan pemrosesan atau dapat diprogram untuk memungkinkan pengguna untuk melakukan pekerjaan. Klien harus mendapatkan kepemilikan untuk setiap Perangkat Klien yang beroperasi, menyediakan data untuk, menggunakan layanan yang diberikan oleh, atau sebaliknya mengakses SaaS IBM selama periode pengukuran yang ditetapkan dalam Dokumen Transaksi Klien.

3. Biaya dan Penagihan

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

3.1 Biaya Pertengahan Bulan (*Partial Month Charges*)

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

4. Kepatuhan dan Audit

Akses ke tawaran IBM Security Trusteer Fraud Protection tunduk pada jumlah maksimum Peserta yang Memenuhi Syarat atau Perangkat Klien sebagaimana yang ditetapkan dalam Dokumen Transaksi. Klien bertanggung jawab untuk memastikan bahwa jumlah Peserta yang Memenuhi Syarat atau Perangkat Klien mereka tidak melebihi jumlah maksimum sebagaimana yang ditetapkan dalam Dokumen Transaksi.

Audit dapat dilakukan untuk memverifikasi kepatuhan terhadap jumlah maksimum Peserta yang Memenuhi Syarat atau Perangkat Klien.

5. Opsi Pembaruan Periode Langganan SaaS IBM

Dokumen Transaksi Klien akan menetapkan apakah SaaS IBM akan diperbarui pada akhir Periode Langganan, dengan menentukan salah satu dari yang berikut:

5.1 Pembaruan Otomatis

Jika Dokumen Transaksi Klien menyatakan bahwa pembaruan Klien adalah otomatis, Klien dapat mengakhiri Periode Langganan SaaS IBM yang habis masa berlakunya dengan permintaan tertulis kepada perwakilan penjualan IBM Klien atau Mitra Bisnis IBM, selambat-lambatnya sembilan puluh (90) hari sebelum tanggal habis masa berlaku jangka waktu sebagaimana yang tercantum dalam Dokumen Transaksi. Jika IBM atau Mitra Bisnis IBM tidak menerima pemberitahuan pengakhiran tersebut sampai dengan tanggal habis masa berlaku, Periode Langganan yang habis masa berlakunya akan diperpanjang secara otomatis baik untuk satu tahun atau durasi yang sama dengan Periode Langganan asli sebagaimana yang tercantum dalam Dokumen Transaksi.

5.2 Penagihan Berkelanjutan

Jika Dokumen Transaksi menyatakan bahwa pembaruan Klien adalah berkelanjutan, Klien akan terus memiliki akses ke SaaS IBM dan akan ditagih atas penggunaan SaaS IBM berdasarkan penagihan berkelanjutan. Untuk mengakhiri penggunaan SaaS IBM dan menghentikan proses penagihan berkelanjutan, Klien akan perlu untuk memberikan pemberitahuan tertulis dalam jangka waktu sembilan puluh (90) hari sebelumnya kepada IBM atau Mitra Bisnis IBM yang meminta pembatalan SaaS IBM Klien. Setelah pembatalan akses Klien, Klien akan ditagih atas setiap biaya akses yang tertunggak selama bulan saat pembatalan berlaku.

5.3 Diperlukan Pembaruan

Jika Dokumen Transaksi menyatakan bahwa pembaruan Klien adalah "berakhir", SaaS IBM akan berakhir pada akhir Periode Langganan dan akses Klien ke SaaS IBM akan dihapus. Agar dapat terus menggunakan SaaS IBM setelah tanggal berakhir, Klien akan perlu untuk memesan ke perwakilan penjualan IBM Klien atau Mitra Bisnis IBM untuk membeli Periode Langganan yang baru.

6. Dukungan Teknis

Dukungan Teknis untuk SaaS IBM tersedia untuk Klien dan Peserta yang Memenuhi Syarat mereka untuk membantu dalam penggunaan mereka atas SaaS IBM.

Dukungan Standar termasuk dalam langganan semua tawaran. Trusteer Rapport Mandatory Service, yang merupakan add-on untuk Rapport Trusteer, memiliki prasyarat Dukungan Premium untuk langganan Rapport Trusteer dasar.

Untuk masing-masing tawaran SaaS IBM, langganan Dukungan Premium tersedia dengan biaya tambahan, dengan pengecualian tawaran IBM Security Trusteer Mobile SDK dan tawaran Layanan Wajib IBM Security Trusteer Rapport.

Dukungan Standar:

- waktu lokal dukungan 08:00-17:00.
- Klien dan Peserta yang Memenuhi Syarat mereka, dapat mengajukan tiket dukungan secara elektronik, sebagaimana yang diuraikan secara rinci dalam Buku Pedoman Dukungan Perangkat Lunak Sebagai Layanan [*Software as a Service* - "SaaS"].
- Klien dapat mengakses Portal Dukungan Klien untuk pemberitahuan, dokumen, laporan kasus dan FAQ di:http://www-01.ibm.com/software/security/trusteer/support/.
- Untuk opsi dukungan dan rincian Pelanggan dapat mengakses Buku Pedoman Dukungan Perangkat Lunak sebagai Layanan [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

Dukungan Premium:

- Dukungan 24x7 untuk semua tingkat permasalahan.
- Klien dapat mencapai dukungan langsung melalui telepon.
- Klien dan Peserta yang Memenuhi Syarat mereka, dapat mengajukan tiket dukungan secara elektronik, sebagaimana yang dijelaskan secara rinci dalam Buku Pedoman Dukungan Perangkat Lunak Sebagai Layanan [*Software as a Service* - "SaaS"].
- Klien dapat mengakses Portal Dukungan Klien untuk pemberitahuan, dokumen, laporan kasus dan FAQ di:http://www-01.ibm.com/software/security/trusteer/support/.
- Untuk opsi dukungan dan rincian Pelanggan dapat mengakses Buku Pedoman Dukungan Perangkat Lunak sebagai Layanan [SaaS]: http://www-01.ibm.com/software/support/handbook.html.

7. Syarat-syarat Tambahan Tawaran SaaS IBM

7.1 Kepatuhan Safe Harbor

IBM mematuhi U.S. – EU Safe Harbor Framework sebagaimana yang dikembangkan oleh Departemen Perdagangan Amerika Serikat berkoordinasi dengan Komisi Eropa. Produk-produk IBM Security Trusteer tercakup dalam sertifikasi EU-U.S. Safe Harbor IBM. Informasi lebih lanjut mengenai Safe Harbor dan daftar perusahaan Safe Harbor dapat ditemukan di sini: http://export.gov/safeharbor/.

7.2 Kenaikan Biaya Langganan Tahunan Klien

IBM berhak untuk menyesuaikan biaya langganan untuk SaaS IBM tidak lebih dari sekali setiap dua belas (12) bulan dengan persentase yang akan ditentukan oleh IBM tidak melebihi 3%. Penyesuaian biaya langganan akan mulai berlaku pada tanggal peringatan (tanggal yang sama pada tahun berikutnya) dari tanggal awal dimulainya periode cakupan.Penyesuaian biaya ini tidak mengubah kepemilikan Klien untuk SaaS IBM atau biaya metrik yang olehnya SaaS IBM diperoleh. Mitra Bisnis IBM merupakan bagian terpisah dari IBM dan dapat menentukan harga dan persyaratan mereka secara sepihak.

7.3 Dukungan Premium

Klien berhak atas Dukungan Premium hanya untuk tawaran SaaS IBM yang untuknya Klien telah berlangganan untuk tawaran Dukungan Premium terkait.

7.4 Persetujuan dan Penggunaan yang Sah Secara Hukum

Otorisasi untuk Mengumpulkan dan Memproses Data

SaaS IBM dirancang untuk membantu Klien meningkatkan lingkungan keamanan dan datanya. SaaS IBM akan mengumpulkan informasi dari Peserta yang Memenuhi Syarat dan Perangkat Klien yang berinteraksi dengan Aplikasi Ritel atau Bisnis yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM. SaaS IBM mengumpulkan informasi yang secara sendiri atau gabungan dapat dianggap Informasi Pribadi dalam beberapa yurisdiksi. Data Pribadi adalah setiap informasi yang dapat digunakan untuk mengidentifikasi individu tertentu, seperti nama, alamat *email*, alamat rumah, atau nomor telepon yang diberikan kepada IBM untuk disimpan, diproses, atau ditransfer atas nama Klien.

Praktik pengumpulan dan pengolahan data dapat diperbarui untuk meningkatkan fungsi dari SaaS IBM. Dokumen dengan uraian lengkap dari praktik pengumpulan dan pengolahan data diperbarui sesuai kebutuhan dan tersedia untuk Klien sesuai permintaan. Klien memberi wewenang kepada IBM untuk mengumpulkan informasi ini dan memrosesnya sesuai dengan pasal Transfer Lintas Batas dan pasal Kerahasiaan Data dari ToU ini, dan pasal Kerahasiaan Data dan Keamanan Data dari Syarat-syarat Umum ToU.

Untuk tawaran IBM Security Trusteer Pinpoint:

Data yang dikumpulkan dapat mencakup alamat IP pengguna, ID pengguna yang diperkecil satu arah atau dienkripsi, domain *cookies* jika tidak disaring, kunjungan ke Aplikasi yang dilindungi dan situs phishing, lokasi geografis dan kredensial yang dimasukkan ke dalam situs *phishing*.

Untuk tawaran IBM Security Trusteer Mobile dan tawaran IBM Security Trusteer Mobile Browser:

Data yang dikumpulkan dapat mencakup alamat IP pengguna, ID pengguna yang diperkecil satu arah atau dienkripsi, lokasi geografis, dan kunjungan ke Aplikasi yang dilindungi, dan afiliasi klien.

Untuk tawaran IBM Security Trusteer Rapport:

Data yang dikumpulkan dapat mencakup alamat IP pengguna, ID pengguna yang diperkecil satu arah atau dienkripsi, peristiwa keamanan, nama pengguna dan alamat *email* yang diberikan untuk tujuan menghubungi IBM untuk dukungan Klien, Afiliasi klien, kata sandi terenkripsi yang dimasukkan di situs yang dilindungi, kunjungan ke Aplikasi yang dilindungi dan situs *phishing*, nomor kartu pembayaran yang dienkripsi, dan berkas dan data yang dikumpulkan dari jarak jauh oleh personel IBM untuk memeriksa dugaan malware yang dicurigai, aktivitas berbahaya, atau kegagalan fungsi.

Persetujuan yang Diinformasikan dari Subjek Data:

Penggunaan SaaS IBM ini dapat melibatkan berbagai peraturan perundang-undangan atau regulasi. SaaS IBM hanya dapat digunakan untuk tujuan yang sah dan dengan cara yang sah menurut hukum. Klien setuju untuk menggunakan SaaS IBM sesuai dengan, dan bertanggung jawab penuh untuk mematuhi, hukum, regulasi, dan kebijakan yang berlaku.

Untuk tawaran IBM Security Trusteer Pinpoint dan tawaran IBM Security Trusteer Mobile SDK:

Klien setuju bahwa pihaknya telah memperoleh atau akan mendapatkan perizinan, lisensi atau persetujuan yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan yang sah secara hukum atas SaaS IBM dan untuk memungkinkan pengumpulan dan pengolahan informasi oleh IBM melalui SaaS IBM.

Untuk tawaran IBM Security Trusteer Rapport dan untuk & tawaran IBM Security Trusteer Mobile Browser:

Klien memberikan wewenang kepada IBM untuk mendapatkan persetujuan yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan yang sah secara hukum atas SaaS IBM dan untuk mengumpulkan dan memroses informasi sebagaimana yang diuraikan dalam Perjanjian Lisensi Pengguna Akhir yang tersedia dihttps://www.trusteer.com/support/end-user-license-agreement. Jika Klien menentukan bahwa pihaknya (dan bukan IBM) akan menangani komunikasi persetujuan dengan pengguna akhir, Klien setuju bahwa pihaknya telah memperoleh atau akan mendapatkan perizinan, lisensi, atau persetujuan, perizinan, atau lisensi yang diinformasikan sepenuhnya yang diperlukan untuk memungkinkan penggunaan yang sah secara hukum atas SaaS IBM dan mengizinkan pengumpulan dan pengolahan informasi oleh IBM sebagai prosesor data Pelanggan melalui SaaS IBM.

7.5 Transfer Lintas Batas

Klien setuju bahwa IBM dapat memroses Konten, termasuk setiap Data Pribadi, berdasarkan peraturan perundang-undangan dan persyaratan yang relevan lintas batas suatu negara ke prosesor dan sub-prosesor di negara berikut di luar Wilayah Ekonomi Eropa dan negara-negara yang dianggap oleh Komisi Eropa memiliki tingkat keamanan yang memadai: Amerika Serikat.

7.6 Kerahasiaan Data

Apabila Klien menyediakan Data Pribadi kepada SaaS IBM di Negara Anggota Uni Eropa, Islandia, Liechtenstein, Norwegia, atau Swiss, atau apabila Klien memiliki Peserta yang Memenuhi Syarat atau Perangkat Klien di negara-negara tersebut, maka Klien sebagai satu-satunya pengendali menunjuk IBM sebagai prosesor untuk mengolah (sebagaimana istilah-istilah tersebut didefinisikan dalam EU Directive 95/46/EC) Data Pribadi. IBM hanya akan mengolah Data Pribadi tersebut sejauh yang diperlukan untuk menyediakan tawaran SaaS IBM sesuai dengan uraian yang diterbitkan oleh IBM mengenai SaaS IBM dan Klien menyetujui bahwa setiap pengolahan tersebut sesuai dengan instruksi Klien. IBM akan memberikan pemberitahuan sebelumnya secara wajar jika IBM melakukan perbuahan material atas lokasi pengolahan atau caranya mengamankan Data Pribadi sebagai bagian SaaS IBM. Klien dapat mengakhiri Periode Langganan saat ini untuk SaaS IBM yang terpengaruh, dengan menyampaikan pemberitahuan tertulis kepada IBM dalam jangka waktu tiga puluh (30) hari sejak IBM menyampaikan pemberitahuan mengenai perubahan kepada Klien. Klien menyetujui bahwa IBM dapat mengolah konten termasuk Data Pribadi apa pun melintasi batas negara kepada prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi*
Entitas IBM yang mengadakan kontrak	Prosesor	Sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services LLC	Sub-prosesor	410 Terry Ave. N Seattle, WA 98109 Amerika Serikat

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi*
Connectria Corp.	Sub-prosesor	10845 Olive Blvd., Suite 300 St. Louis, MO 63141 Amerika Serikat
IBM Israel Ltd.	Sub-prosesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel
IBM Corp	Sub-prosesor	1 New Orchard Rd. Armonk, NY 10504 Amerika Serikat

Klien menyetujui bahwa IBM dapat, dengan pemberitahuan, mengubah daftar lokasi negara ini ketika ditentukan secara wajar bahwa hal ini diperlukan untuk penyediaan SaaS IBM.

Klien setuju bahwa untuk layanan yang disediakan melalui pusat data Jerman, sebagaimana yang ditentukan dalam proses penetapan, IBM dapat mengolah konten termasuk Data Pribadi apa pun melintasi batas negara kepada prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi*
Entitas IBM yang mengadakan kontrak	Prosesor	Sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services (Jerman)	Sub-prosesor	Munich, Jerman
IBM Israel Ltd.	Sub-prosesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

Klien menyetujui bahwa untuk layanan yang disediakan melalui pusat data Jepang, sebagaimana yang ditentukan dalam proses penyediaan, IBM dapat mengolah konten termasuk Data Pribadi apa pun melintasi batas negara kepada prosesor dan sub-prosesor berikut ini:

Nama Prosesor/Sub-prosesor	Peran (Prosesor atau Sub-prosesor Data)	Lokasi*
Entitas IBM yang mengadakan kontrak	Prosesor	Sebagaimana yang dinyatakan dalam Dokumen Transaksi
Amazon Web Services (Jepang)	Sub-prosesor	Tokyo, Jepang
IBM Israel Ltd.	Sub-prosesor	94 Derech Em-Hamoshavot 49527 Petach-Tikva Israel

* Lokasi tersebut yang diidentifikasikan dalam tabel di atas termasuk alamat kantor perusahaan Prosesor/Sub-prosesor. Pusat data berlokasi di dalam negara yang sama yang diidentifikasikan.

Para pihak atau afiliasi mereka yang relevan dapat mengadakan perjanjian EU Model Clause standar secara terpisah yang tidak dimodifikasi dalam peran mereka yang terkait sesuai dengan EC Decision 2010/87/EU dengan menghapus klausa opsional. Semua sengketa atau tanggung jawab yang timbul berdasarkan perjanjian ini, bahkan apabila diadakan oleh para afiliasi, akan diperlakukan oleh para pihak seolah-olah sengketa atau tanggung jawab tersebut timbul di antara mereka berdasarkan syarat-syarat Perjanjian ini.

Apendiks A

1. Tawaran SaaS IBM

IBM menawarkan layanan ini sebagai layanan dan tawaran berdiri sendiri, atau layanan dan tawaran tambahan. Tawaran SaaS IBM spesifik yang dipesan ditetapkan dalam PoE Klien.

1.1 Definisi Ritel dan Bisnis

Produk-produk cacat IBM Security Trusteer dilisensikan untuk digunakan dengan jenis Aplikasi spesifik. Aplikasi ditentukan sebagai salah satu jenis berikut: Ritel atau Bisnis. Tawaran terpisah tersedia untuk Aplikasi Ritel dan Aplikasi Bisnis.

- Aplikasi Ritel didefinisikan sebagai suatu aplikasi *online* banking, aplikasi *mobile* atau aplikasi e-commerce yang dirancang untuk melayani konsumen. Kebijakan Klien dapat mengklasifikasikan usaha kecil tertentu sebagai memenuhi syarat untuk akses ritel.
- Aplikasi Bisnis didefinisikan sebagai sebuah aplikasi *online* banking, aplikasi *mobile* atau aplikasi e-commerce yang dirancang untuk melayani korporasi, institusi, atau yang setara, atau aplikasi apa pun yang tidak dikategorikan sebagai Ritel.

1.2 Tawaran Langganan Dasar SaaS IBM

Tawaran Bisnis:

- IBM Security Trusteer Rapport for Business
- IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Business
- IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile
- IBM Security Trusteer Mobile SDK for Business
- IBM Security Trusteer Mobile Browser for Business

Tawaran Ritel:

- IBM Security Trusteer Rapport for Retail
- IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Security Trusteer Pinpoint Criminal Detection for Retail
- IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile
- IBM Security Trusteer Mobile SDK for Retail
- IBM Security Trusteer Mobile Browser for Retail

Untuk masing-masing tawaran Bisnis dan Ritel, tersedia produk Dukungan Premium dengan biaya tambahan, dengan pengecualian tawaran IBM Security Trusteer Mobile SDK.

1.3 Tawaran Langganan SaaS IBM tambahan untuk IBM Security Trusteer Rapport

Tawaran tambahan tersedia untuk IBM Security Trusteer Rapport untuk Bisnis:

- IBM Security Trusteer Rapport Fraud Feeds for Business
- IBM Security Trusteer Rapport Phishing Protection for Business
- IBM Security Trusteer Rapport Mandatory Service for Business

Tawaran tambahan tersedia untuk IBM Security Trusteer Rapport untuk Ritel:

- IBM Security Trusteer Rapport Fraud Feeds for Retail
- IBM Security Trusteer Rapport Phishing Protection for Retail
- IBM Security Trusteer Rapport Mandatory Service for Retail

Untuk masing-masing *add-on* Bisnis dan Ritel pada tawaran IBM Security Trusteer Rapport, kecuali untuk add-on IBM Security Trusteer Rapport Mandatory Service, tersedia produk Dukungan Premium terkait dengan biaya tambahan.

Langganan IBM Security Trusteer Rapport for Business atau IBM Security Trusteer Rapport for Retail merupakan prasyarat untuk tambahan tawaran Langganan SaaS IBM terkait yang tercantum dalam pasal ini.

1.4 Tawaran Langganan SaaS IBM tambahan untuk Tawaran IBM Security Trusteer Pinpoint Malware Detection

Tersedia tawaran tambahan untuk IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition atau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Business

Tersedia tawaran tambahan untuk IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition atau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition:

- IBM Security Trusteer Pinpoint Carbon Copy for Retail
- IBM Security Trusteer Rapport Remediation for Retail

Tersedia langganan Dukungan Premium dengan biaya tambahan untuk setiap tawaran SaaS IBM tambahan yang tercantum dalam pasal ini.

Langganan tawaran IBM Security Trusteer Pinpoint Malware Detection for Business atau tawaran IBM Security Trusteer Pinpoint Malware Detection for Retail merupakan prasyarat untuk tambahan tawaran langganan SaaS IBM terkait yang tercantum dalam pasal ini.

1.5 Langganan SaaS IBM Tambahan Lainnya

Setiap Langganan SaaS IBM tambahan untuk langganan dasar di atas yang tidak tercantum dalam dokumen ini, baik saat ini tersedia atau dalam pengembangan, tidak dianggap pembaruan dan harus diberikan secara terpisah.

1.6 Definisi

Pemegang Akun – adalah pengguna akhir dari Klien, yang telah memasang perangkat lunak klien yang diaktifkan, yang menerima perjanjian lisensi pengguna akhir ("EULA"), dan dikonfirmasi setidaknya sekali dengan Ritel Klien atau Aplikasi Bisnis di mana untuknya Klien telah berlangganan untuk cakupan SaaS IBM.

Perangkat Lunak Klien Pemegang Akun – berarti perangkat lunak klien-diaktifkan IBM Security Trusteer Rapport atau perangkat lunak klien-diaktifkan IBM Security Trusteer Mobile Browser atau perangkat lunak yang diaktifkan oleh Klien lainnya yang disediakan dengan beberapa langganan SaaS IBM untuk pemasangan pada perangkat pengguna akhir.

Trusteer Splash – mengacu pada *splash* yang diberikan kepada Klien berdasarkan templat *splash* yang tersedia.

Halaman Arahan – mengacu ke halaman yang diadakan oleh IBM yang diberikan kepada Klien dengan splash Klien dan Perangkat Lunak Klien Pemegang Akun yang dapat diunduh.

2. Tawaran IBM Security Trusteer Rapport

2.1 IBM Security Trusteer Rapport for Retail dan/atau IBM Security Trusteer Rapport for Business ("Trusteer Rapport")

Trusteer Rapport memberikan lapisan perlindungan terhadap *phishing* dan serangan *malware* Man-in-the-Browser (MITB). Menggunakan jaringan puluhan juta titik akhir di seluruh dunia IBM Security Trusteer Rapport mengumpulkan keterangan-keterangan mengenai *phishing* dan serangan *malware* aktif terhadap organisasi di seluruh dunia. IBM Security Trusteer Rapport menggunakan algoritma perilaku yang bertujuan untuk memblokir serangan *phishing* dan untuk mencegah pemasangan dan pengoperasian strain *malware* MITB.

Tawaran SaaS IBM ini memiliki metrik biaya Peserta yang Memenuhi Syarat. Tawaran Bisnis dijual dalam paket 10 Peserta yang Memenuhi Syarat. Tawaran Ritel dijual dalam paket 100 Peserta yang Memenuhi Syarat.

Tawaran SaaS IBM ini termasuk:

a. Aplikasi Trusteer Management ("TMA"):

   TMA tersedia pada lingkungan yang di-*hosting* oleh cloud IBM Security Trusteer, yang melaluinya Klien (dan personelnya yang berwenang yang tidak terbatas jumlahnya) dapat: (i) menerima pelaporan data peristiwa dan penilaian risiko, (ii) melihat, mengonfigurasi, dan mengatur kebijakan dan kebijakan yang berkaitan dengan pelaporan data peristiwa, dan (iii) mengonfigurasi pengoperasian perangkat lunak klien yang diaktifkan berlisensi untuk publik berdasarkan perjanjian lisensi pengguna akhir ("EULA") tanpa biaya, dan disediakan untuk diunduh ke desktop atau perangkat Peserta yang Memenuhi Syarat (PC/Mac), juga dikenal sebagai rangkaian perangkat lunak Trusteer Rapport ("Perangkat Lunak Klien Pemegang Akun"). Klien hanya dapat memasarkan perangkat Lunak Klien Pemegang Akun yang menggunakan TrusteerSplash atau Rapport API, dan Klien tidak dapat menggunakan Perangkat Lunak Klien Pemegang Akun untuk operasi bisnis internal atau penggunaan karyawannya (selain penggunaan pribadi karyawan).

b. Skrip *Web*:

   Untuk akses pada situs web dengan tujuan mengakses atau menggunakan tawaran SaaS IBM.

c. Data peristiwa:

   Klien (dan personelnya yang berwenang yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari Perangkat Lunak Klien Pemegang Akun sebagai akibat dari interaksi *online* Pemegang Akun dengan Aplikasi Bisnis atau Ritel yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM. Data peristiwa akan diterima dari Perangkat Lunak Klien Pemegang Akun Peserta yang Memenuhi Syarat yang berjalan pada perangkat mereka, yang telah menerima EULA, dikonfirmasi dengan Aplikasi Bisnis atau Ritel Klien setidaknya sekali, dan konfigurasi Klien harus mencakup kumpulan ID Pengguna.

d. Trusteer Splash:

   Platform pemasaran Trusteer Splash mengidentifikasi dan memasarkan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan untuk cakupan tawaran SaaS IBM. Klien dapat memilih dari Templat Splash yang tersedia. Splash kustomisasi dapat dikontrak berdasarkan perjanjian atau pernyataan kerja yang terpisah.

Klien dapat setuju untuk memberikan merek dagang, logo, atau lambangnya untuk penggunaan yang terkait dengan TMA dan hanya untuk penggunaan dengan Trusteer Splash dan untuk ditampilkan di Perangkat Lunak Klien Pemegang Akun atau pada halaman arahan yang di-*hosting* oleh IBM dan pada situs *we*b IBM Security Trusteer. Setiap penggunaan merek dagang, logo, atau lambang yang diberikan akan sesuai dengan kebijakan yang wajar dari IBM mengenai iklan dan penggunaan merek dagang.

Klien harus berlangganan tawaran SaaS IBM Security Trusteer Rapport Mandatory Service jika ingin menggunakan jenis penyebaran wajib Perangkat Lunak Klien Pemegang Akun.

Penyebaran wajib Perangkat Lunak Klien Pemegang Akun termasuk namun tidak terbatas pada, semua jenis penyebaran wajib oleh mekanisme atau alat yang secara langsung atau tidak langsung memaksa Peserta yang Memenuhi Syarat untuk mengunduh Perangkat Lunak Klien Pemegang Akun, mencegah akses ke Aplikasi Bisnis dan/atau Ritel Pelanggan jika Perangkat Lunak Klien Pemegang Akun tidak dipasang, atau metode apa pun yang membedakan fitur Pemegang Akun dari Peserta yang Memenuhi Syarat Pelanggan lainnya, atau metode apa pun yang dibuat untuk mengabaikan persyaratan lisensi penyebaran wajib Perangkat Lunak Klien Pemegang Akun ini, atau alat, prosedur, kebijakan, perjanjian, atau mekanisme apa pun yang tidak dibuat oleh atau disetujui oleh IBM untuk digunakan dalam penyebaran tidak wajib Perangkat Lunak Klien Pemegang Akun.

2.2 Tambahan Opsional Tawaran SaaS IBM untuk IBM Security Trusteer Rapport for Business dan/atau IBM Security Trusteer Rapport for Retail

Langganan tawaran IBM Security Trusteer Rapport merupakan prasyarat untuk berlangganan ke salah satu tawaran SaaS IBM tambahan setelahnya. Jika SaaS IBM ditetapkan sebagai "*for Business* ", maka tawaran SaaS IBM tambahan yang diperoleh juga harus ditunjuk sebagai "*for Business*". Jika SaaS IBM ditetapkan sebagai "*for Retail*", maka tawaran SaaS IBM tambahan yang diperoleh juga harus ditetapkan sebagai "*for Retail*". Klien akan menerima data peristiwa dari Peserta yang Memenuhi Syarat yang menjalankan Perangkat Lunak Klien Pemegang Akun yang telah menerima EULA, dikonfirmasi dengan

Aplikasi Bisnis dan/atau Aplikasi Ritel Klien setidaknya sekali, dan konfigurasi Klien harus mencakup kumpulan ID Pengguna.

2.2.1 IBM Security Trusteer Rapport Fraud Feeds for Business dan/atau IBM Security Trusteer Rapport Fraud Feeds for Retail

Klien (dan personelnya yang berwenang yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang berkaitan dengan infeksi *malware* dan kerentanan titik akhir lainnya pada desktop Pemegang Akun tertentu.

2.2.2 IBM Security Trusteer Rapport Phishing Protection for Business dan/atau IBM Security Trusteer Rapport Phishing Protection for Retail

Klien (dan personelnya yang berwenang yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima pemberitahuan data peristiwa yang berkaitan dengan penyerahan kredensial login Pemegang Akun untuk *phishing* atau situs yang berpotensi penipuan. Aplikasi *online* yang sah (URL) mungkin keliru ditandai sebagai situs *phishing* dan SaaS IBM dapat mengingatkan Pemegang Akun bahwa situs yang sah tersebut adalah situs *phishing*. Dalam hal tersebut, Klien harus memberitahu IBM mengenai kesalahan tersebut, dan IBM akan memperbaiki kesalahan tersebut. Ini akan menjadi satu-satunya perbaikan Klien untuk kesalahan tersebut.

2.2.3 IBM Security Trusteer Rapport Mandatory Service for Business dan/atau IBM Security Trusteer Rapport Mandatory Service for Retail

Klien dapat menggunakan suatu mesin virtual dari *platform* pemasaran Trusteer Splash untuk mewajibkan mengunduh Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan cakupan Layanan SaaS IBM.

IBM Security Trusteer Rapport Premium Support for Business merupakan prasyarat untuk IBM Security Rapport Mandatory Service for Business.

IBM Security Trusteer Rapport Premium Support for Retail merupakan prasyarat untuk IBM Security Rapport Mandatory Service for Retail.

Klien dapat menerapkan fungsi tambahan IBM Security Trusteer Rapport Mandatory Service hanya jika diperintahkan dan dikonfigurasi untuk digunakan dengan Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM.

3. Tawaran IBM Security Trusteer Pinpoint

IBM Security Trusteer Pinpoint adalah layanan berbasis cloud yang dirancang untuk memberikan lapisan perlindungan lain dan bertujuan untuk mendeteksi dan mengurangi *malware*, *phishing* dan serangan pengambilalihan akun. Trusteer Pinpoint dapat diintegrasikan ke dalam Aplikasi Bisnis dan/atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan pada cakupan tawaran SaaS IBM dan proses pencegahan penipuan.

Tawaran SaaS IBM ini termasuk:

a. TMA:

   TMA tersedia pada lingkungan yang di-*hosting* oleh cloud IBM Security Trusteer, yang melaluinya Klien (dan personelnya yang berwenenang yang tidak terbatas jumlahnya) dapat: (i) menerima pelaporan data peristiwa dan penilaian risiko, dan (ii) melihat, mengonfigurasi, dan mengatur kebijakan keamanan dan kebijakan yang berkaitan dengan pelaporan data peristiwa.

b. Skrip Web dan/atau API:

   Untuk penyebaran pada situs web untuk tujuan mengakses atau menggunakan SaaS IBM.

3.1 IBM Security Trusteer Pinpoint Malware Detection dan IBM Security Trusteer Pinpoint Criminal Detection

Dalam hal deteksi *malware* pada tawaran IBM Security Trusteer Pinpoint Malware Detection atau deteksi risiko pada tawaran IBM Security Trusteer Pinpoint Criminal Detection, Klien harus mengikuti Panduan Praktek Terbaik Pinpoint. Jangan menggunakan tawaran IBM Security TrusteerPinpoint Malware Detection atau tawaran IBM Security TrusteerPinpoint Criminal Detection dengan cara apa pun yang akan mempengaruhi pengalaman Peserta yang Memenuhi Syarat segera setelah deteksi *malware*, sedemikian rupa sehingga akan memungkinkan yang lain untuk menghubungkan tindakan Klien dengan menggunakan tawaran IBM Security TrusteerPinpoint Malware Detection (misalnya, pemberitahuan,

pesan, memblokir perangkat, atau memblokir akses ke Aplikasi Bisnis dan/atau Aplikasi Ritel segera setelah deteksi *malware*).

3.1.1 IBM Security Trusteer Pinpoint Criminal Detection for Business dan/atau IBM Security Trusteer Pinpoint Criminal Detection for Retail

Pendeteksian Clientless dari aktivitas pengambilalihan akun yang mencurigakan dari browser yang menghubungkan ke Aplikasi Bisnis atau Aplikasi Ritel, menggunakan ID perangkat, deteksi *phishing*, dan deteksi pencuri kredensial berbasis *malware*. Tawaran IBM Security Trusteer Pinpoint Criminal Detection menyediakan lapisan perlindungan lain dan bertujuan untuk mendeteksi upaya pengambilalihan akun dan memberikan skor penilaian risiko browser atau perangkat *mobile* (melalui browser asli atau aplikasi *mobile* Klien) yang mengakses Aplikasi Bisnis atau Aplikasi Ritel secara langsung ke Klien.

a. Data peristiwa:

Klien (dan personelnya yang sah yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi *online* Peserta yang Memenuhi Syarat dengan Aplikasi Bisnis dan/atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM atau Klien dapat menerima data peristiwa melalui mode pengiriman API backend.

3.1.2 IBM Security Trusteer Pinpoint Criminal Detection for Business Mobile dan/atau IBM Security Trusteer Pinpoint Criminal Detection for Retail Mobile

Tawaran IBM Security Trusteer Pinpoint Criminal detection for Mobile (PPCD Mobile) dirancang untuk memberikan lapisan perlindungan lain dan bertujuan untuk melindungi dari pengambilalihan akun dan kegiatan penipuan dengan mengidentifikasi akses akun kriminal dan menyediakan rekomendasi kepada klien. Tawaran SaaS IBM ini mengumpulkan informasi yang datang baik dari Aplikasi Bisnis dan/atau Aplikasi Ritel Klien dengan menggunakan PPCD Mobile API, dan dari Perangkat *mobile* Peserta yang Memenuhi Syarat. Tawaran IBM Security Trusteer PPCD Mobile dirancang untuk menghubungkan informasi kompleks yang terkait dengan Perangkat *mobile* Peserta yang Memenuhi Syarat, dengan sumber data lain, seperti infeksi *malware* waktu nyata dan insiden *phishing* yang terintegrasi melalui tawaran SaaS IBM lainnya dari IBM Security Trusteer yang ditetapkan dalam TOU ini.

Klien dapat mengakses dan menggunakan tawaran IBM Security Trusteer PPCD Mobile pada lingkungan yang di-hosting oleh cloud IBM Security Trusteer dan menerima data penilaian risiko dari perangkat *mobile* Peserta yang Memenuhi Syarat, yang dihasilkan sebagai hasil dari interaksi *online* perangkat *mobile* ini dengan Aplikasi Bisnis atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM. Untuk tujuan tawaran ini, "perangkat *mobile*" hanya termasuk ponsel dan tablet dan tidak termasuk PC laptop atau MAC.

3.1.3 IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Pendeteksian *Clientless browser* yang terinfeksi *malware* finansial Man in the Browser (MiTB) yang menghubungkan ke Aplikasi Bisnis dan/atau Aplikasi Ritel. Tawaran IBM SecurityTrusteer Pinpoint Malware Detection memberikan lapisan perlindungan lain dan bertujuan untuk memungkinkan organisasi untuk fokus pada proses pencegahan penipuan berdasarkan risiko *malware* dengan menyediakan penilaian dan peringatan bagi Klien akan keberadaan *malware* finansial MiTB.

a. Data peristiwa:

Klien (dan personelnya yang berwenang yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan dari interaksi *online* Peserta yang Memenuhi Syarat dengan Aplikasi Bisnis dan/atau Aplikasi Ritel Klien.

b. Edisi Lanjutan:

Edisi Lanjutan untuk Bisnis dan/atau Ritel memberikan lapisan tambahan deteksi dan perlindungan yang disesuaikan dan dikustomisasi pada struktur dan alur Aplikasi Bisnis dan/atau Ritel Klien, dan dapat disesuaikan dengan lanskap ancaman spesifik yang menarget Klien. Hal ini dapat dimasukkan di berbagai lokasi pada Aplikasi Bisnis dan/atau Ritel Klien.

Edisi Lanjutan ditawarkan dalam jumlah minimum kepada Klien setidaknya 100K Peserta yang Memenuhi Syarat Ritel atau 10K Peserta yang Memenuhi Syarat Bisnis, yang berisi 1000 paket 100

Peserta yang Memenuhi Syarat untuk Ritel, atau 1000 paket 10 Peserta yang Memenuhi Syarat untuk Bisnis.

c. Edisi Standar:

Edisi Standar untuk Bisnis atau untuk Ritel adalah solusi cepat untuk menyebarkan yang menyediakan fungsionalitas inti dari tawaran SaaS IBM ini seperti yang diuraikan di sini.

3.2 Tambahan Opsional Tawaran SaaS IBM untuk IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition dan/atau IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition

Untuk IBM Security Trusteer Rapport Remediation untuk tawaran Ritel, terdapat prasyarat IBM Security Trusteer Pinpoint Malware Detection for Retail Standard edition atau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition.

Untuk IBM Security Trusteer Pinpoint Carbon Copy for Retail, terdapat prasyarat IBM Security Trusteer Pinpoint Malware Detection for Retail Standard Edition atau IBM Security Trusteer Pinpoint Malware Detection for Retail Advanced Edition. Untuk IBM Security Trusteer Pinpoint Carbon Copy for Business, terdapat prasyarat IBM Security Trusteer Pinpoint Malware Detection for Business Standard Edition atau IBM Security Trusteer Pinpoint Malware Detection for Business Advanced Edition.

3.2.1 IBM Security Trusteer Pinpoint Carbon Copy for Business dan/atau IBM Security Trusteer Pinpoint Carbon Copy for Retail

Tawaran IBM Security Trusteer Pinpoint Carbon Copy dirancang untuk memberikan lapisan perlindungan lain dan layanan pemantauan yang dapat membantu mengidentifikasi jika kredensial Peserta yang Memenuhi Syarat ini telah terancam oleh serangan Phishing pada Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM.

3.2.2 IBM Security Trusteer Rapport Remediation for Retail

IBM Security Trusteer Rapport Remediation for Retail bertujuan untuk menyelidiki, memulihkan, memblokir, dan menghapus infeksi *malware* man-in-the-browser (MiTB) dari perangkat yang terinfeksi (PC/Mac) Peserta yang Memenuhi Syarat Klien yang mengakses Aplikasi Ritel Klien berbasis ad-hoc, di mana infeksi *malware* MiTB telah terdeteksi oleh data peristiwa IBM Security Trusteer Pinpoint Malware Detection. Klien harus memiliki langganan saat ini untuk IBM Security Trusteer Pinpoint Malware Detection yang benar-benar berjalan pada Aplikasi Ritel Klien. Klien dapat menggunakan tawaran SaaS IBM ini hanya bersama dengan Peserta yang Memenuhi Syarat yang mengakses Aplikasi Ritel Klien, dan semata-mata sebagai alat yang bertujuan untuk menyelidiki dan memulihkan perangkat yang terinfeksi tertentu (PC/MAC) secara *ad-hoc*. IBM Security Trusteer Rapport Remediation for Retail harus benar-benar berjalan pada perangkat (PC/MAC) Peserta yang Memenuhi Syarat tersebut yang terinfeksi, dan Peserta yang Memenuhi Syarat yang terinfeksi tersebut harus menerima EULA, mengotentikasi dengan Aplikasi Ritel Klien setidaknya sekali, dan konfigurasi Klien harus termasuk kumpulan ID Pengguna. Untuk menghindari keraguan, tawaran SaaS IBM ini tidak termasuk hak untuk menggunakan Trusteer Splash dan/atau mempromosikan Perangkat Lunak Klien Pemegang Akun dengan cara lain untuk populasi umum Peserta yang Memenuhi Syarat Klien.

4. Tawaran IBM Security Trusteer Mobile

4.1 IBM Security Trusteer Mobile Browser for Business dan/atau IBM Security Trusteer Mobile Browser for Retail

IBM Security Trusteer Mobile Browser dirancang untuk menambah lapisan lain perlindungan dan bertujuan untuk menyediakan akses *online* yang aman dari perangkat *mobile* Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis atau Aplikasi Ritel Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM, penilaian risiko perangkat *mobile*, dan perlindungan *phishing*. Deteksi Wi-Fi aman hanya tersedia untuk *platform* Android. Untuk tujuan tawaran SaaS IBM ini termasuk perangkat *mobile* termasuk ponsel atau tablet dan tidak termasuk PC Laptop dan Mac.

Melalui TMA, Klien (dan personilnya yang berwenang yang tidak terbatas jumlahnya) dapat menerima data peristiwa, analisis, dan informasi statistik yang berkaitan dengan Perangkat di mana Peserta yang Memenuhi Syarat telah: (i) mengunduh Perangkat Lunak Klien Pemegang Akun, suatu aplikasi yang dilisensikan untuk publik berdasarkan perjanjian lisensi pengguna akhir ("EULA") tanpa biaya, dan dibuat tersedia untuk mengunduh ke perangkat *mobile* Peserta yang Memenuhi Syarat, dan (ii) menerima EULA

dan diotentikasi setidaknya sekali dengan Aplikasi Bisnis atau Ritel Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM. Klien hanya dapat memasarkan Perangkat Lunak Klien Pemegang Akun menggunakan Trusteer Splash dan tidak dapat menggunakan Perangkat Lunak Klien Pemegang Akun untuk operasi bisnis internalnya.

a. Data peristiwa:

   Klien (dan personelnya yang sah yang jumlahnya tidak terbatas) dapat menggunakan TMA untuk menerima data peristiwa yang dihasilkan sebagai hasil dari interaksi *online* perangkat *mobile* dengan Aplikasi Ritel atau Bisnis Klien yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM.

b. Trusteer Splash:

   Platform pemasaran Trusteer Splash mengidentifikasi dan memasarkan Perangkat Lunak Klien Pemegang Akun kepada Peserta yang Memenuhi Syarat yang mengakses Aplikasi Bisnis dan/atau Ritel Klien yang untuknya Klien telah berlangganan untuk cakupan tawaran SaaS IBM. Klien dapat memilih dari templat *splash* yang tersedia ("Templat *Splash*"). *Splash* kustomisasi dapat dikontrak berdasarkan perjanjian atau pernyataan kerja yang terpisah.

Klien dapat setuju untuk memberikan merek dagang, logo, atau lambangnya untuk penggunaan yang terkait dengan TMA dan hanya untuk penggunaan dengan Trusteer Splash dan untuk ditampilkan di Perangkat Lunak Klien Pemegang Akun atau pada halaman arahan yang di-*hosting* oleh IBM atau pada situs web IBM Security Trusteer. Setiap penggunaan merek dagang, logo, atau lambang yang diberikan akan sesuai dengan kebijakan IBM yang wajar mengenai iklan dan penggunaan merek dagang.

4.2 IBM Security Trusteer Mobile SDK for Business dan/atau IBM Security Trusteer Mobile SDK for Retail

Tawaran IBM Security Trusteer Mobile SDK dirancang untuk menambah lapisan perlindungan lain untuk menyediakan akses web yang aman ke Aplikasi Bisnis dan/atau Aplikasi Ritel Ritel yang untuknya Ritel telah berlangganan cakupan tawaran SaaS IBM, penilaian risiko perangkat, dan perlindungan *pharming*. Deteksi Wi-Fi aman hanya tersedia untuk *platform* Android.

Tawaran IBM Security Trusteer Mobile SDK termasuk alat pengembang perangkat lunak ("SDK") *mobile* hak milik, sebuah paket perangkat lunak yang berisi dokumentasi, pustaka perangkat lunak hak milik pemrograman serta item dan file terkait lainnya, yang dikenal sebagai pustaka *mobile* IBM Security Trusteer serta " Komponen *Run-time*", atau " *Redistributable*", kode hak milik yang dihasilkan oleh IBM Security Trusteer Mobile SDK yang dapat tertanam dan diintegrasikan ke dalam aplikasi *mobile* iOS atau Android Klien yang berdiri sendiri yang dilindungi yang untuknya Klien telah berlangganan cakupan tawaran SaaS IBM.("Aplikasi *Mobile* Terpadu Klien").

IBM Security Trusteer Mobile SDK for Retail tersedia dalam paket 100 Peserta yang Memenuhi Syarat atau paket dari 100 Perangkat Klien, dan IBM Security Trusteer Mobile SDK for Business tersedia dalam paket 10 Peserta yang Memenuhi Syarat atau paket dari 10 Perangkat Klien.

Melalui TMA, Klien (dan sebanyak mungkin personil berwenang) dapat menerim pelaporan data peristiwa dan penilaian kecenderungan risiko. Melalui Aplikasi *Mobile* Terpadu Klien, Klien dapat menerima data peristiwa, analisis, dan statistik informasi yang berkaitan dengan perangkat *mobile* Peserta yang Memenuhi Syarat yang telah mengunduh Aplikasi *Mobile* Terpadu Klien. Untuk tujuan tawaran ini, "perangkat *mobile*" hanya termasuk ponsel dan tablet serta tidak termasuk PC laptop atau MAC.

Klien dapat:

a. secara internal menggunakan IBM Security Trusteer Mobile SDK semata-mata untuk tujuan mengembangkan Aplikasi *Mobile* Terpadu Klien;

b. menanamkan *Redistributable* (hanya dalam format kode objek), sebagai cara yang tidak terpisahkan dalam Aplikasi *Mobile* Terpadu Klien. Setiap bagian yang diubah atau digabung dari *Redistributable* yang sesuai untuk pemberian lisensi ini tunduk terhadap syarat TOU ini; dan

c. memasarkan dan mendistribusikan *Redistributable* untuk unduhan pada perangkat *mobile* Peserta yang Memenuhi Syarat atau pada pemegang Perangkat Klien, dengan ketentuan bahwa:

   - Kecuali sebagaimana yang diizinkan dalam Perjanjian ini, Klien tidak dapat (1) menggunakan, menyalin, memodifikasi, atau mendistribusikan SDK; (2) merakit balik, mengompilasi balik, atau sebaliknya menerjemahkan, atau merekayasa balik SDK, kecuali sebagaimana yang diizinkan oleh hukum tanpa kemungkinan pembebasan kontrak; (3) mensublisensikan, menyewakan, atau menyewa SDK, (4) memindahkan satiap hak cipta atau menandai file yang

terdapat dalam *Redistributable*; (5) menggunakan jalur yang sama dengan file/modul *Redistributable*; dan (6) menggunakan nama atau merek dagang IBM, penerima lisensinya, atau distributornya sehubungan dengan pemasaran Aplikasi *Mobile* Terintegrasi Klien tanpa izin tertulis sebelumnya dari IBM penerima lisensinya atau distributornya.

- *Redistributable* harus tetap terintegrasi dalam cara yang tidak dapat dipisahkan dalam Aplikasi *Mobile* Terintegrasi Klien. *Redistributable* harus berupa bentuk kode objek dan harus sesuai dengan semua panduan, petunjuk, dan spesifikasi dalam SDK dan dokumentasinya. Perjanjian lisensi pengguna akhir untuk Aplikasi *Mobile* Terintegrasi Klien harus memberitahu pengguna akhir bahwa *Redistributable* atau modifikasinya tidak boleh i) digunakan untuk tujuan apa pun selain untuk mengaktifkan Aplikasi *Mobile* Terintegrasi Klien, ii) disalin (kecuali untuk tujuan cadangan), iii) didistribusikan lebih lanjut atau ditransfer iv) direkayasa balik, disusun balik, atau diterjemahkan lain kecuali sebagaimana yang diizinkan secara spesifik oleh hukum dan tanpa kemungkinan terdapat adanya pengabaian kontraktual. Perjanjian lisensi Klien harus setidaknya sebagai pelindung dari IBM sebagai ketentuan Perjanjian ini.
- SDK dapat hanya disebarkan sebagai bagian dari pengembangan internal Klien dan pengujian unit pada perangkat pengujian *mobile* Klien yang ditentukan. Klien tidak berwenang untuk menggunakan SDK untuk memproses beban kerja produksi, mensimulasikan beban kerja produksi atau menguji skalabilitas kode, aplikasi atau sistem apa pun. Klien tidak berwenang untuk menggunakan setiap bagian dari SDK untuk tujuan lain apa pun.

Klien bertanggung jawab atas semua bantuan teknis untuk Aplikasi Mobile Terintegrasi Klien dan setiap modifikasi pada *Redistributable* yang dilakukan oleh Klien sebagaimana yang diizinkan dalam dokumen ini.

Klien berwenang untuk memasang dan menggunakan Redistributable dan IBM Security Mobile SDK hanya untuk mendukung penggunaan Klien atas tawaran SaaS IBM.

IBM telah menguji contoh aplikasi yang dibuat dengan alat *mobile* yang tersedia dalam IBM Security Trusteer Mobile SDK ("*Mobile Tool*") untuk menentukan apakah mereka akan mengeksekusi dengan baik pada versi tertentu dari *platform* sistem operasi *mobile* dari Apple (iOS), Google (Android), dan lain-lain (secara bersama-sama "Platform OS Mobile"), namun, Platform OS Mobile yang disediakan oleh pihak ketiga, tidak berada di bawah kendali IBM dan dapat berubah tanpa pemberitahuan kepada IBM. Dengan demikian, dan tanpa mengindahkan ketentuan apa pun yang mengatur sebaliknya, IBM tidak menjamin bahwa setiap aplikasi atau *output* lain yang dibuat dengan menggunakan Peralatan *Mobile* akan berjalan dengan baik pada, beroperasi bersama atau kompatibel dengan Platform OS Mobile atau perangkat *mobile* apa pun.

Klien setuju untuk menciptakan, menyimpan, dan memberikan kepada IBM dan auditornya, catatan akurat tertulis, *output* alat sistem, dan informasi sistem lainnya yang cukup untuk memberikan verifikasi yang dapat diaudit bahwa penggunaan Klien atas IBM Security Trusteer Mobile SDK sesuai dengan ketentuan ToU ini.

5. Penyebaran Tawaran IBM SaaS Fraud Protection

Langganan dasar Klien meliputi pengaturan yang diperlukan dan kegiatan penyebaran awal, termasuk startup satu kali awal, konfigurasi, Templat Splash, pengujian, dan pelatihan.

Layanan tambahan dapat dikontrak untuk biaya tambahan dengan perjanjian terpisah.

Apendiks B

IBM menyediakan perjanjian tingkat layanan ("SLA") ketersediaan berikut untuk SaaS IBM dan berlaku jika ditetapkan dalam Dokumen Transaksi Klien:

Versi SLA ini, yaitu yang terbaru saat dimulainya atau pembaruan jangka waktu langganan Klien akan berlaku. Klien memahami bahwa SLA bukan merupakan suatu jaminan untuk Klien.

1. Definisi

a. **Kontak yang Sah** – adalah individu yang telah ditetapkan Klien kepada IBM yang diberi wewenang untuk mengajukan Klaim berdasarkan Perjanjian Tingkat Layanan ini.

b. **Kredit yang Tersedia** – adalah ganti rugi yang akan diberikan oleh IBM untuk Klaim yang telah divalidasi. Kredit yang Tersedia akan diterapkan dalam bentuk kredit atau diskon pada faktur biaya langganan yang akan datang untuk SaaS IBM.

c. **Klaim –** adalah klaim yang diajukan oleh Kontak Klien yang Sah kepada IBM berdasarkan SLA ini bahwa suatu Tingkat Layanan belum dipenuhi selama suatu Bulan Masa Kontrak.

d. **Bulan Masa Kontrak** – adalah setiap bulan penuh selama jangka waktu SaaS IBM yang dihitung dari pukul 00:00 GMT pada tanggal pertama suatu bulan sampai pukul 23:59 GMT pada tanggal terakhir bulan tersebut.

e. **Klien** – adalah entitas yang berlangganan untuk SaaS IBM secara langsung dari IBM, dan yang tidak dalam keadaan wanprestasi atas kewajiban material apa pun, termasuk kewajiban pembayaran, berdasarkan kontrak dengan IBM untuk SaaS IBM.

f. **Waktu Henti** – adalah periode waktu di mana pemrosesan sistem produksi untuk Layanan telah berhenti dan semua pengguna Anda tidak dapat menggunakan semua aspek Layanan yang untuknya mereka memiliki izin-izin yang tepat. Waktu Henti tidak termasuk periode waktu pada saat Layanan tidak tersedia sebagai akibat dari:

- Waktu Henti Sistem yang Direncanakan;
- Keadaan Kahar;
- Permasalahan-permasalahan dengan aplikasi, peralatan atau data Klien atau pihak ketiga;
- Tindakan atau kelalaian Klien maupun pihak ketiga (termasuk siapa pun yang mendapatkan akses ke SaaS IBM melalui kata sandi atau peralatan Klien);
- Ketidakmampuan untuk mematuhi konfigurasi sistem yang disyaratkan dan *platform* yang didukung untuk mengakses SaaS IBM; atau
- Kepatuhan IBM terhadap setiap desain, spesifikasi atau instruksi yang diberikan oleh Klien atau pihak ketiga atas nama Klien.

g. **Peristiwa –** adalah keadaan atau serangkaian keadaan yang bersama-sama menyebabkan kegagalan untuk memenuhi suatu Tingkat Layanan.

h. **Keadaan Kahar** – adalah bencana alam, terorisme, aksi buruh, kebakaran, banjir, gempa bumi, huru-hara, perang, tindakan, peraturan atau pembatasan dari Pemerintah, virus, serangan DoS dan perbuatan merugikan lainnya, kerusakan utilitas dan konektivitas jaringan atau setiap penyebab lain dari ketidaktersediaan SaaS IBM yang berada di luar kendali IBM secara wajar.

i. **Waktu Henti Sistem yang Direncanakan** – adalah penghentian SaaS IBM yang terjadwal untuk tujuan pemeliharaan.

j. **Tingkat Layanan –** adalah standar yang tercantum di bawah ini yang digunakan IBM untuk mengukur tingkat layanan yang diberikannya dalam SLA ini.

2. Kredit yang Tersedia

a. Guna memenuhi persyaratan untuk mengajukan Klaim, Klien harus mencatatkan tiket dukungan untuk setiap Peristiwa dengan bagian bantuan (*helpdesk*) dukungan pelanggan IBM untuk SaaS IBM yang berlaku, sesuai dengan prosedur IBM untuk pelaporan masalah dukungan Tingkat Permasalahan 1. Klien harus menyediakan semua informasi rinci yang diperlukan tentang Peristiwa dan membantu IBM secara wajar dengan diagnosis dan resolusi Peristiwa sejauh diperlukan untuk

tiket dukungan Tingkat Permasalahan 1. Tiket tersebut harus dicatatkan dalam waktu dua puluh empat (24) jam sejak Klien pertama kali menyadari bahwa Peristiwa tersebut telah berdampak pada penggunaan Klien atas SaaS IBM.

b. Kontak Klien yang Sah harus mengajukan Klaim Klien untuk Kredit yang Tersedia selambat-lambatnya dalam jangka waktu tiga (3) hari kerja setelah akhir Bulan Masa Kontrak yang merupakan pokok Klaim.

c. Kontak Resmi Klien harus memberikan kepada IBM semua rincian yang wajar mengenai Klaim, termasuk namun tidak terbatas pada, uraian rinci dari semua Peristiwa yang relevan dan Tingkat Layanan yang diklaim belum dipenuhi.

d. IBM akan mengukur total kombinasi Waktu Henti secara internal selama setiap Bulan Masa Kontrak yang berlaku untuk Tingkat Layanan yang sesuai dengan yang tertera dalam tabel di bawah ini. Kredit yang Tersedia akan didasarkan pada durasi Waktu Henti yang diukur dari saat Klien melaporkan bahwa Klien tersebut pertama kali terkena dampak dari Waktu Henti. Apabila Klien melaporkan Peristiwa Waktu Henti Aplikasi dan Peristiwa Waktu Henti Pemrosesan Data yang Masuk yang terjadi secara serentak, maka IBM akan memperlakukan periode Waktu Henti yang tumpang tindih sebagai suatu periode Waktu Henti tunggal, dan bukan sebagai dua periode Waktu Henti yang terpisah. Untuk masing-masing Klaim yang sah, IBM akan memberlakukan Kredit yang Tersedia yang berlaku paling tinggi berdasarkan Tingkat Layanan yang dicapai selama setiap Bulan Masa Kontrak, sebagaimana yang tertera dalam tabel-tabel di bawah ini. IBM tidak akan bertanggung jawab atas beberapa Kredit yang Tersedia untuk Peristiwa(-peristiwa) yang sama dalam Bulan Masa Kontrak yang sama.

e. Untuk Layanan yang Dibundel (SaaS IBM individu yang dipaket dan dijual bersama-sama dengan harga kombinasi tunggal), Kredit yang Tersedia akan dihitung berdasarkan harga kombinasi tunggal bulanan untuk Layanan yang Dibundel, dan bukan biaya langganan bulanan untuk setiap SaaS IBM individu. Klien hanya dapat mengajukan Klaim yang berkaitan dengan satu SaaS IBM individu dalam suatu bundel dalam setiap Bulan Masa Kontrak, dan IBM tidak akan bertanggung jawab atas Kredit yang Tersedia yang berkaitan dengan lebih dari satu SaaS IBM dalam suatu bundel dalam Bulan Masa Kontrak mana pun.

f. Jika Klien membeli SaaS IBM dari penjual kembali IBM yang sah dalam transaksi pemasaran kembali dimana IBM mempertahankan tanggung jawab utama untuk memenuhi komitmen-komitmen SaaS IBM dan Perjanjian Tingkat Layanan, Kredit yang Tersedia akan didasarkan pada *Relationship Suggested Value Price* (RSVP) yang berlaku pada saat itu untuk SaaS IBM yang berlaku selama Bulan Masa Kontrak yang merupakan pokok Klaim, didiskon sebesar 50%.

g. Total Kredit yang Tersedia yang diberikan berkaitan dengan Bulan Masa Kontrak mana pun tidak akan, dalam keadaan apa pun, melebihi sepuluh persen (10%) dari satu per dua belas (1/12) dari biaya tahunan yang dibayar oleh Klien kepada IBM untuk SaaS IBM.

h. IBM akan menggunakan penilaiannya yang wajar untuk memvalidasi Klaim berdasarkan informasi yang tersedia dalam catatan IBM, yang akan berlaku apabila terjadi ketidaksesuaian dengan data pada catatan Klien.

i. KREDIT YANG TERSEDIA YANG DIBERIKAN UNTUK KLIEN SESUAI DENGAN SLA INI ADALAH GANTI RUGI PELANGGAN SATU-SATUNYA DAN YANG EKSKLUSIF YANG BERKAITAN DENGAN KLAIM APA PUN.

3. Tingkat Layanan

Ketersediaan SaaS IBM selama suatu Bulan Masa Kontrak

Tingkat Layanan yang Dicapai (selama suatu Bulan Masa Kontrak)	**Kredit yang Tersedia (% dari Biaya Langganan Bulanan untuk Bulan Masa Kontrak yang merupakan pokok Klaim)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

"Tingkat Layanan yang Dicapai", dinyatakan dalam persentase, dihitung sebagai: (a) jumlah menit dalam suatu Bulan Masa Kontrak, dikurangi (b) jumlah menit Waktu Henti di dalam suatu Bulan Masa Kontrak, dibagi dengan (c) jumlah menit dalam suatu Bulan Masa Kontrak.

Contoh: 250 menit total Waktu Henti selama Bulan Masa Kontrak

43.200 total menit dalam suatu Bulan Masa Kontrak selama 30 hari - Waktu Henti 250 menit = 42.950 menit Total 43.200 menit	= 2% dari Kredit yang Tersedia untuk 99,4% Tingkat Layanan yang Dicapai selama Bulan Masa Kontrak

3.1 Pengecualian

Perjanjian Tingkat Layanan ini disediakan hanya untuk Klien IBM. Perjanjian Tingkat Layanan ini tidak berlaku untuk hal-hal berikut:

- Layanan Beta dan uji coba.
- Lingkungan non-produksi, termasuk namun tidak terbatas pada, pengujian, pemulihan bencana, uji mutu (*quality assurance*), atau pengembangan.
- Klaim yang dibuat oleh pengguna, tamu, peserta, dan pihak yang diizinkan oleh Klien IBM yang menggunakan SaaS IBM.
- Jika Klien telah melanggar kewajiban material apa pun berdasarkan ToU, termasuk namun tidak terbatas kepada, pelanggaran kewajiban pembayaran apa pun.

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.