Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila timbul perbedaan, ketidakkonsistenan, atau pertentangan antara terjemahan dan versi bahasa Inggris (khususnya karena keterlambatan penerjemahan), versi bahasa Inggris akan berlaku.

KEBIJAKAN KEAMANAN VENDOR

Terakhir diperbarui 28 Januari 2022

1. CAKUPAN; DEFINISI.

1.1 Kebijakan Keamanan. Pemasok dalam segala hal akan mematuhi persyaratan keamanan informasi Amazon yang ditetapkan dalam kebijakan ini ("**Kebijakan Keamanan**"). Kebijakan Keamanan ini berlaku terhadap kinerja Pemasok berdasarkan Perjanjian serta seluruh akses, pengumpulan, penggunaan, penyimpanan, pemindahan, pengungkapan, penghancuran, atau penghapusan, serta insiden keamanan Pemasok terkait Informasi Amazon. Kebijakan Keamanan tidak membatasi kewajiban lain Pemasok, termasuk kewajiban berdasarkan segala perjanjian lain dengan Amazon atau undang-undang lain yang berlaku terhadap Pemasok, kinerja Pemasok berdasarkan perjanjian lain dengan Amazon, Informasi Amazon, atau Tujuan yang Diizinkan. Apabila Kebijakan Keamanan ini bertentangan dengan perjanjian larangan pengungkapan antara para pihak, atau segala perjanjian lain yang berlaku terhadap para pihak, Pemasok akan segera memberi tahu Amazon tentang pertentangan tersebut dan mematuhi persyaratan yang lebih melindungi Informasi Amazon, kecuali jika persyaratan yang kurang melindungi tersebut secara tegas dinyatakan mengesampingkan persyaratan yang lebih melindungi (yang dapat ditetapkan oleh Amazon). Amazon dapat mengubah Kebijakan Keamanan ini dari waktu ke waktu, dengan ketentuan bahwa jika perubahan tersebut tidak wajar secara komersial, atas permintaan Amazon, akan bertemu dan menyetujui biaya tambahan yang sesuai.

1.2 Definisi.

1.2.1 "**Agregat**" berarti menggabungkan atau menyimpan Informasi Amazon dengan data atau informasi Pemasok atau pihak ketiga mana pun.

1.2.2 "**Perjanjian**" berarti perjanjian apa pun yang merujuk pada Kebijakan Keamanan ini.

1.2.3 "**Amazon**" berarti Amazon.com, Inc. dan afiliasinya.

1.2.4 "**Anonimisasi**" berarti menggunakan, mengumpulkan, menyimpan, mentransmisikan, atau mengubah data atau informasi apa pun (termasuk Informasi Amazon) dengan cara atau bentuk yang tidak mengidentifikasi, mengizinkan identifikasi, dan tidak berkaitan dengan Amazon, atau pengguna, pengidentifikasi perangkat, sumber, produk, layanan, konteks, atau merek apa pun darinya.

1.2.5 "**Informasi Amazon**" berarti secara individu dan bersama-sama: (a) seluruh Informasi Rahasia Amazon (sebagaimana ditetapkan dalam perjanjian larangan pengungkapan atau perjanjian lain antara para pihak); (b) seluruh data, catatan, file, konten, atau informasi lainnya, dalam bentuk atau format apa pun, yang diperoleh, diakses, dikumpulkan, diterima, disimpan, atau dipelihara oleh Pemasok atau afiliasinya, dari atau atas nama Amazon, atau sehubungan dengan Kebijakan Keamanan ini atau layanan, atau kinerja atau pelaksanaan hak para pihak berdasarkan atau sehubungan dengan Perjanjian; dan (c) informasi yang berasal dari (a) atau (b), sekalipun Dianonimkan.

1.2.6 "Pemasok" berarti setiap Pemasok, Vendor, atau Kontraktor yang ditetapkan dalam Perjanjian dan penyedia lainnya sesuai dengan Perjanjian.

1.3 Tujuan yang Diizinkan. Pemasok dapat mengakses, mengumpulkan, menggunakan, menyimpan, dan mentransmisikan Informasi Amazon saja yang secara tegas diizinkan berdasarkan Perjanjian dan semata-mata hanya untuk tujuan menyediakan produk atau layanan berdasarkan Perjanjian, sesuai dengan lisensi yang diberikan (jika ada) berdasarkan Kebijakan Keamanan ini ("**Tujuan yang Diizinkan**"). Kecuali jika secara tegas

diizinkan berdasarkan Perjanjian, Pemasok tidak akan mengakses, mengumpulkan, menggunakan, menyimpan, atau mentransmisikan Informasi Amazon apa pun dan tidak akan Mengagregatkan Informasi Amazon, sekalipun Dianonimkan. Kecuali dengan persetujuan tertulis tegas Amazon sebelumnya, Pemasok tidak akan (a) mengalihkan, menyewakan, menukar, memperdagangkan, menjual, meminjamkan, atau menyewagunakan, atau mendistribusikan atau menyediakan Informasi Amazon kepada pihak ketiga mana pun, atau (b) Mengagregatkan Informasi Amazon dengan informasi atau data lain apa pun, sekalipun Dianonimkan.

2. KEBIJAKAN KEAMANAN AMAZON.

2.1 Persyaratan Keamanan Dasar. Pemasok akan, sesuai dengan standar industri terbaik saat ini dan persyaratan lainnya yang ditetapkan oleh Amazon berdasarkan klasifikasi dan sensitivitas Informasi Amazon, memelihara pengamanan fisik, administrasi, dan teknis serta langkah keamanan lainnya untuk (a) memelihara keamanan dan kerahasiaan Informasi Amazon yang diakses, dikumpulkan, digunakan, disimpan, atau ditransmisikan oleh Pemasok, dan (b) melindungi informasi tersebut dari ancaman atau bahaya yang diketahui atau diperkirakan secara wajar terhadap keamanan dan integritas, kehilangan yang tidak disengaja, perubahan, dan pengungkapan, serta bentuk pemrosesan lain yang melanggar hukum. Tanpa batasan, Pemasok akan mematuhi persyaratan berikut untuk segala sistem yang digunakan Pemasok untuk memproses Informasi Amazon atau yang dapat mengakses Informasi Amazon ("**Sistem Informasi Amazon**"):

2.1.1 Keamanan Jaringan. Pemasok akan melindungi segala Sistem Informasi Amazon dengan membatasi akses jaringan tanpa izin, khususnya dari Internet eksternal. Pemasok akan menginstal dan memelihara solusi keamanan jaringan yang efektif, seperti firewall, untuk senantiasa melindungi Informasi Amazon.

2.1.2 Pembaruan. Sebagaimana dijabarkan dalam Badan Nasional Standar dan Publikasi Khusus (Special Publication atau "SP") 800-40 Revisi 3 Teknologi Amerika Serikat (National Institute of Standards and Technology atau "NIST"), Pemasok akan terus memperbarui Sistem Informasi Amazon dengan peningkatan, pembaruan, perbaikan bug, dan versi baru terkini serta modifikasi lainnya yang diperlukan untuk memastikan keamanan Informasi Amazon.

2.1.3 Antimalware. Pemasok akan senantiasa menggunakan perangkat lunak antimalware atau pengendalian keamanan yang setara untuk menanggulangi risiko penyusupan dan penyebaran malware. Apabila digunakan, Pemasok akan terus memperbarui perangkat lunak antimalware.

2.1.4 Enkripsi. Pemasok akan mengenkripsi data yang tiba di tujuan dan data yang dikirimkan di seluruh jaringan terbuka sesuai dengan praktik terbaik industri.

2.1.5 Pengujian. Pemasok akan menguji sistem dan proses keamanannya secara berkala untuk memastikan semuanya memenuhi persyaratan Kebijakan Keamanan ini atau kebijakan keamanan yang sebelumnya disetujui oleh Pemasok dan Amazon. Sejauh terdapat perubahan terhadap Kebijakan Keamanan sesuai dengan Bagian 1.1, perubahan tersebut tidak akan berlaku untuk tujuan Bagian ini hingga terdapat kesepakatan antara Pemasok dan Amazon (email sudah memadai).

2.1.6 Pengendalian Akses. Pemasok akan mengamankan Informasi Amazon, termasuk dengan mematuhi persyaratan berikut:

2.1.6.1 Pemasok akan menetapkan ID unik kepada setiap orang yang memiliki akses komputer ke Informasi Amazon atau Sistem Informasi Amazon.

2.1.6.2 Pemasok akan membatasi akses ke Informasi Amazon kepada mereka "yang perlu mengetahuinya" untuk Tujuan yang Diizinkan.

2.1.6.3 Pemasok akan meninjau daftar orang dan layanan yang memiliki akses ke Informasi Amazon secara berkala dan menghapus akun yang tidak lagi memerlukan akses ke Sistem Informasi Amazon. Peninjauan ini harus dilaksanakan setidaknya setiap 90 hari sekali.

2.1.6.4 Pemasok tidak akan menggunakan kata sandi sistem dan parameter keamanan bawaan lain dari produsen pada Sistem Informasi Amazon. Pemasok akan mewajibkan dan memastikan penggunaan "kata sandi yang kuat" yang diterapkan sistem sesuai dengan praktik terbaik yang dijelaskan dalam NIST SP 800-63B pada seluruh Sistem Informasi Amazon. Pemasok akan

mewajibkan semua kata sandi dan kredensial akses dirahasiakan dan tidak dibagikan di antara personel.

2.1.6.5 Pemasok akan memelihara dan memberlakukan "penguncian akun" dengan menonaktifkan akun dengan akses ke Informasi Amazon atau Sistem Informasi Amazon saat akun tersebut memiliki lebih dari sepuluh (10) percobaan kata sandi salah secara berturut-turut.

2.1.6.6 Kecuali jika secara tegas diizinkan oleh Amazon secara tertulis, Pemasok akan senantiasa secara fisik atau logis memisahkan Informasi Amazon (termasuk dalam penyimpanan, pemrosesan, atau transmisi) dari informasi Pemasok dan pihak ketiga mana pun.

2.1.6.7 Apabila pengendalian akses fisik tambahan diminta secara tertulis oleh Amazon, Pemasok akan menerapkan dan menggunakan langkah pengendalian akses fisik aman tersebut.

2.1.6.8 Pemasok akan menyediakan hal berikut kepada Amazon atas permintaan wajar Amazon, (a) data log tentang seluruh penggunaan akun atau kredensial Amazon (baik yang diizinkan maupun tanpa izin) yang disediakan kepada Pemasok untuk Tujuan yang Diizinkan (misalnya kredensial akun media sosial), dan (b) data log terperinci tentang setiap peniruan identitas, atau percobaan peniruan identitas, personel Amazon atau personel Pemasok yang memiliki akses ke Informasi Amazon.

2.1.6.9 Pemasok akan meninjau log akses secara berkala untuk mencari tanda perilaku berbahaya atau akses tanpa izin.

2.1.7 Kebijakan Pemasok. Pemasok akan memelihara dan memberlakukan kebijakan keamanan informasi dan jaringan untuk karyawan, subkontraktor, agen, dan pemasok yang memenuhi standar yang ditetapkan dalam Kebijakan Keamanan ini, termasuk metode untuk mendeteksi dan mencatat pelanggaran kebijakan. Atas permintaan Amazon, Pemasok akan menyediakan informasi tentang pelanggaran terhadap kebijakan keamanan informasi dan jaringan Pemasok kepada Amazon jika Pemasok atau Amazon memiliki dugaan yang wajar bahwa itu dianggap sebagai Insiden Keamanan (ditetapkan di bawah).

2.1.8 Subkontrak. Pemasok tidak akan melakukan subkontrak atau mendelegasikan kewajibannya berdasarkan Kebijakan Keamanan ini kepada subkontraktor atau delegasi mana pun (secara bersama-sama disebut sebagai "**Subkontraktor**") tanpa persetujuan tertulis Amazon sebelumnya. Tanpa mengabaikan keberadaan atau ketentuan subkontrak atau delegasi mana pun, Pemasok akan tetap bertanggung jawab terhadap pelaksanaan kewajibannya secara menyeluruh berdasarkan Kebijakan Keamanan ini. Syarat dan ketentuan Kebijakan Keamanan ini akan mengikat Subkontraktor dan personel Pemasok. Pemasok akan (a) memastikan bahwa Subkontraktor dan personelnya mematuhi Kebijakan Keamanan ini, dan (b) bertanggung jawab atas seluruh tindakan, kelalaian, keteledoran, serta kesalahan Subkontraktor dan personel Pemasok

2.1.9 Akses Jarak Jauh. Pemasok akan memastikan bahwa segala akses ke Sistem Informasi Amazon memerlukan autentikasi mutlifaktor (misalnya memerlukan setidaknya dua faktor berbeda untuk mengidentifikasi pengguna).

2.1.10 Akses "In Bulk". Untuk tujuan bagian ini, akses "in bulk" berarti mengakses data menggunakan pertanyaan basis data, pembuatan laporan, atau pengalihan data dalam jumlah besar lainnya. Kecuali jika secara tegas diizinkan oleh Amazon secara tertulis, Pemasok tidak akan mengakses, dan tidak akan mengizinkan akses ke, Informasi Amazon secara "in bulk", tanpa memandang jika Informasi Amazon berada dalam basis data yang dikendalikan oleh Pemasok atau Amazon, atau disimpan dalam bentuk lain, termasuk penyimpanan dalam arsip berbasis file (misalnya file datar), dll. Secara khusus, bagian ini melarang segala akses ke Informasi Amazon kecuali untuk akses ke catatan individu sebagaimana diperlukan untuk Tujuan yang Diizinkan. Pemasok akan memelihara data log terperinci tentang percobaan akses atau akses "in bulk" yang berhasil ke Informasi Amazon dan akan menyediakan laporan dari log ini sebagai bagian dari kewajiban Pemasok berdasarkan Bagian 2.5 (Peninjauan Keamanan). Apabila Amazon menyediakan otorisasi tertulis kepada Pemasok untuk akses "in bulk" ke Informasi Amazon, Pemasok akan (a) membatasi akses tersebut hanya kepada karyawan tertentu "yang perlu mengetahuinya", dan (b) menggunakan alat bantu yang membatasi akses serta memerlukan otorisasi eksplisit dan pencatatan semua akses.

2.1.11 Personel Pemasok. Amazon dapat menentukan akses personel Pemasok ke Informasi Amazon pada penandatanganan dan pengiriman perjanjian larangan pengungkapan individu, dalam bentuk yang ditetapkan oleh Amazon, kepada Amazon. Personel Pemasok akan menandatangani perjanjian larangan pengungkapan individu jika Amazon mewajibkannya. Pemasok akan memperoleh dan mengirimkan perjanjian larangan pengungkapan individu yang telah ditandatangani dari personel Pemasok yang akan memiliki akses ke Informasi Amazon (sebelum pemberian akses atau penyediaan informasi kepada personel Pemasok) kepada Amazon. Pemasok juga akan memelihara seluruh daftar personel Pemasok yang telah mengakses atau menerima Informasi Amazon pada Sistem Informasi Amazon serta segera menyediakan daftar tersebut kepada Amazon setelah diminta. Untuk personel Pemasok mana pun yang (a) tidak lagi memerlukan akses ke Informasi Amazon atau (b) tidak memenuhi syarat sebagai personel Pemasok (misalnya individu keluar dari ketenagakerjaan Pemasok), Pemasok akan segera mengakhiri akses (dalam maksimum 24 jam) ke Informasi Amazon dan Sistem Informasi Amazon. Apabila personel tersebut berwenang untuk mengakses Informasi Amazon pada Sistem Informasi Amazon, Pemasok akan memberi tahu Amazon dalam 24 jam.

2.2 Akses ke Ekstranet dan Portal Pemasok Amazon. Amazon dapat memberi Pemasok akses menuju Informasi Amazon melalui portal web atau situs web non-publik atau layanan ekstranet lainnya di situs web atau sistem milik Amazon atau pihak ketiga (masing-masing disebut sebagai "**Ekstranet**") untuk Tujuan yang Diizinkan. Apabila Amazon mengizinkan Pemasok mengakses Informasi Amazon menggunakan Ekstranet, Pemasok harus mematuhi persyaratan berikut:

2.2.1 Tujuan yang Diizinkan. Pemasok dan personel Pemasok akan mengakses Ekstranet dan mengakses, mengumpulkan, menggunakan, melihat, mengambil, mengunduh, atau menyimpan Informasi Amazon dari Ekstranet sepenuhnya hanya demi Tujuan yang Diizinkan.

2.2.2 Akun. Pemasok akan memastikan bahwa personel Pemasok hanya menggunakan akun(-akun) Ekstranet yang ditetapkan Amazon untuk masing-masing individu dan akan mewajibkan personel Pemasok untuk menjaga kerahasiaan kredensial akses mereka.

2.2.3 Sistem. Pemasok akan mengakses Ekstranet hanya melalui sistem atau aplikasi komputasi atau pemrosesan yang menjalankan sistem operasi yang dikelola oleh Pemasok dan yang mencakup: (a) firewall jaringan sistem sesuai dengan Bagian 2.1.1 (Keamanan Jaringan); (b) pengelolaan patch tersentralisasi sesuai dengan Bagian 2.1.2 (Pembaruan); (c) perangkat lunak antimalware yang tepat dengan sistem operasi sesuai dengan Bagian 2.1.3 (Antimalware); dan (d) enkripsi disk penuh untuk perangkat portabel.

2.2.4 Pembatasan. Kecuali jika disetujui sebelumnya secara tertulis oleh Amazon, Pemasok tidak akan mengunduh, mencerminkan, atau secara permanen menyimpan Informasi Amazon dari Ekstranet mana pun pada media apa pun, termasuk setiap mesin, perangkat, atau server.

2.2.5 Pengakhiran Akun. Pemasok akan mengakhiri akun, dan memberi tahu Amazon selambat-lambatnya 24 jam setelah, personel Pemasok mana pun yang berwenang untuk mengakses Ekstranet mana pun: (a) tidak lagi memerlukan akses menuju Informasi Amazon atau (b) tidak lagi berkualifikasi sebagai personel Pemasok (misalnya personel keluar dari ketenagakerjaan dengan Pemasok).

2.2.6 Sistem Pihak Ketiga.

2.2.6.1 Pemasok akan memberi tahu Amazon terlebih dahulu dan menerima persetujuan tertulis Amazon lebih dahulu sebelum menggunakan sistem pihak ketiga apa pun yang menyimpan atau mungkin memiliki akses ke Informasi Amazon, kecuali jika (a) data dienkripsi sesuai dengan Kebijakan Keamanan ini, dan (b) sistem pihak ketiga tidak akan memiliki akses ke kunci dekripsi atau versi "teks polos" tanpa enkripsi dari data tersebut. Amazon berhak untuk mewajibkan peninjauan keamanan Amazon (sesuai dengan Bagian 2.5 (Peninjauan Keamanan)) terhadap sistem pihak ketiga sebelum memberikan persetujuan.

2.2.6.2 Apabila Pemasok menggunakan sistem pihak ketiga yang menyimpan Informasi Amazon yang tidak dienkripsi atau yang dapat mengakses Informasi Amazon yang tidak dienkripsi, Pemasok akan melaksanakan peninjauan keamanan sistem pihak ketiga dan pengendalian keamanannya, serta memberikan laporan berkala kepada Amazon mengenai pengendalian keamanan sistem pihak

ketiga tersebut dalam format yang diminta oleh Amazon (misalnya SAS 70 atau laporan penerusnya, atau laporan standar industri yang dikenali lainnya yang disetujui Amazon).

2.3 Penyimpanan dan Pemusnahan Data.

2.3.1 Penyimpanan. Pemasok akan menyimpan Informasi Amazon hanya untuk tujuan, dan selama diperlukan untuk, Tujuan yang Diizinkan.

2.3.2 Pengembalian atau Penghapusan. Atas permintaan Amazon, Pemasok akan segera (namun tidak lebih dari 72 jam) mengembalikan ke Amazon serta secara permanen dan aman menghapus seluruh Informasi Amazon sesuai dengan pemberitahuan Amazon yang mengharuskan pengembalian dan/atau penghapusan tersebut. Pemasok juga akan secara permanen dan aman menghapus semua contoh langsung (yang dapat diakses secara online atau melalui jaringan) dari Informasi Amazon dalam 30 hari setelah pemenuhan Tujuan yang Diizinkan sebelumnya atau setelah Kebijakan Keamanan ini diakhiri atau kedaluwarsa. Apabila diminta oleh Amazon, Pemasok akan menyatakan secara tertulis bahwa semua Informasi Amazon telah dimusnahkan. Demi kejelasan, bagian ini tidak akan berlaku untuk Salinan Arsip sesuai dengan Bagian 2.3.3

2.3.3 Salinan Arsip. Apabila Pemasok diwajibkan oleh hukum untuk menyimpan salinan arsip Informasi Amazon untuk keperluan pajak atau keperluan regulasi serupa, Informasi Amazon yang diarsipkan ini harus disimpan dalam salah satu dari beberapa cara berikut:

2.3.3.1 Sebagai cadangan “dingin” atau offline (yaitu, tidak dapat diakses untuk penggunaan langsung atau interaktif) yang disimpan dalam fasilitas yang aman secara fisik; atau

2.3.3.2 Dienkripsi, saat sistem yang meng-hosting atau menyimpan file(-file) yang dienkripsi tidak memiliki akses ke salinan kunci(-kunci) yang digunakan untuk enkripsi.

2.3.4 Pemulihan. Apabila Pemasok melakukan “pemulihan” (yaitu, mengembalikan cadangan) demi keperluan pemulihan dari bencana, Pemasok akan mengadakan dan mempertahankan proses yang memastikan semua Informasi Amazon yang perlu dihapus sesuai dengan Perjanjian atau Kebijakan Keamanan ini maupun perjanjian lain dengan Amazon akan dihapus kembali atau ditimpa dari data yang dipulihkan sesuai dengan Bagian 2.3 ini dalam waktu 24 jam setelah pemulihan data dilakukan. Apabila Pemasok melakukan pemulihan demi tujuan apa pun, Informasi Amazon tidak boleh dipulihkan ke sistem atau jaringan pihak ketiga mana pun tanpa persetujuan tertulis Amazon sebelumnya. Amazon berhak mewajibkan peninjauan keamanan Amazon (sesuai dengan Bagian 2.5 (Peninjauan Keamanan)) terhadap sistem atau jaringan pihak ketiga sebelum mengizinkan pemulihan Informasi Amazon ke sistem atau jaringan pihak ketiga mana pun.

2.3.5 Standar Sanitasi Data. Seluruh Informasi Amazon yang dihapus oleh Pemasok akan dihapus sesuai dengan Rekomendasi Sanitasi Minimum yang tercantum dalam NIST SP 800-88 Revisi 1, Pedoman untuk Sanitasi Data, 18 Desember 2014 (tersedia di http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Apendiks A, untuk pembersihan jenis perangkat terkait. Apabila tidak ada pedoman terkait dalam NIST SP 800-88, Apendiks A, perangkat yang berisi Informasi Amazon akan dimusnahkan dalam salah satu cara berikut: (a) melalui demagnetisasi media magnetis pada medan fluks elektromagnet 10.000+ Gauss, (b) dengan memecah atau menghancurkan secara mekanis menjadi partikel yang lebih kecil dari 2x2 mm, atau (c) melalui standar pemusnahan lain yang mungkin diwajibkan Amazon berdasarkan klasifikasi dan sensitivitas Informasi Amazon tersebut.

2.4 Pemusnahan Forensik. Sebelum membuang (dalam cara apa pun) setiap perangkat keras, perangkat lunak, atau media lain yang berisi, atau pernah berisi, Informasi Amazon, Pemasok akan melakukan pemusnahan forensik perangkat keras, perangkat lunak, atau media lain tersebut, yang tidak memungkinkan pengambilan Informasi Amazon tersebut dalam cara apa pun. Pemasok akan melakukan pemusnahan forensik sesuai dengan Rekomendasi Sanitasi Minimum yang tercantum dalam NIST SP 800-88, Apendiks A, untuk memusnahkan jenis perangkat terkait.

2.4.1 Pemasok tidak akan menjual, menjual kembali, mendonasikan, merakit kembali, atau mengalihkan (termasuk setiap penjualan atau pengalihan perangkat keras, perangkat lunak, atau media lainnya, penempatan apa pun sehubungan dengan likuidasi bisnis Pemasok, atau penempatan lain) perangkat

keras, perangkat lunak, atau media lain yang berisi Informasi Amazon yang belum dimusnahkan secara forensik oleh Pemasok sebagaimana diwajibkan di Bagian 2.4 ini.

2.5 Peninjauan Keamanan.

2.5.1 Amazon berhak untuk secara berkala meminta Pemasok untuk berpartisipasi dalam penilaian risiko Amazon.

2.5.2 Sertifikasi. Atas permintaan tertulis Amazon, Pemasok akan menyatakan kepada Amazon secara tertulis bahwa informasi yang diberikan sebagai bagian dari penilaian risiko mematuhi Kebijakan Keamanan ini yang terakhir disetujui oleh Pemasok dan Amazon. Sejauh terdapat perubahan terhadap Kebijakan Keamanan sesuai dengan Bagian 1.1, perubahan tersebut tidak akan berlaku untuk tujuan Bagian ini hingga terdapat kesepakatan antara Pemasok dan Amazon (email sudah memadai).

2.5.3 Peninjauan Lain. Amazon berhak untuk secara berkala meninjau keamanan Sistem Informasi Amazon, tetapi tidak lebih dari sekali setahun kecuali jika (a) terdapat kekurangan substansial yang teridentifikasi dalam tahun kalender tersebut atau (b) Amazon diwajibkan oleh badan pemerintah atau badan regulasi lain untuk melaksanakan peninjauan tersebut. Pemasok akan bekerja sama dan memberi Amazon semua informasi yang diperlukan dalam jangka waktu yang wajar namun tidak lebih dari 20 hari kalender sejak tanggal permintaan Amazon.

2.5.4 Remediasi. Apabila peninjauan keamanan mengidentifikasi kekurangan apa pun, Pemasok akan, dengan biaya dan pengeluaran Pemasok sendiri, melakukan semua tindakan wajar yang diperlukan untuk memulihkan semua kekurangan tersebut dalam jangka waktu yang disepakati.

2.6 Insiden Keamanan.

2.6.1 Pemasok akan memberi tahu Amazon sesegera mungkin, namun tidak lebih dari 24 jam, setelah Pemasok mengetahui setiap akses, pengumpulan, perolehan, penggunaan, transmisi, pengungkapan tanpa izin, kerusakan, atau kehilangan Informasi Amazon atau pelanggaran setiap Sistem Informasi Amazon yang sudah atau diduga terjadi ("**Insiden Keamanan**"). Pemasok akan memulihkan setiap Insiden Keamanan secara tepat waktu dan memberikan perincian tertulis kepada Amazon mengenai penyelidikan internal Pemasok terkait dengan masing-masing Insiden Keamanan. Apabila diizinkan oleh undang-undang yang berlaku, Pemasok setuju untuk tidak memberi tahu setiap badan regulasi atau pelanggan atas nama Amazon, kecuali jika secara khusus diminta oleh Amazon secara tertulis agar Pemasok melakukannya, dan Amazon berhak untuk meninjau dan menyetujui bentuk dan isi pemberitahuan apa pun sebelum diberikan kepada pihak mana pun. Pemasok akan bekerja sama dengan Amazon untuk menyusun dan melaksanakan rencana demi memperbaiki semua Insiden Keamanan yang sudah dikonfirmasi.

2.6.2 Sejauh diizinkan oleh hukum yang berlaku, jika Pemasok menerima permintaan atau perintah dari badan pemerintah (seperti panggilan, perintah pengadilan, atau surat izin penggeledahan) yang meminta data yang mencakup Informasi Amazon apa pun, Pemasok akan memberikan pemberitahuan yang memadai kepada Amazon demi memungkinkan Amazon untuk mengupayakan perintah perlindungan atau tindakan pemulihan lain yang sesuai.

2.7 Umum. Amazon memiliki pertimbangan mutlak dalam mengambil semua keputusan yang dapat diterapkan berdasarkan Kebijakan Keamanan ini. Setiap daftar contoh yang didahului kata "termasuk" atau "misalnya" bersifat ilustratif dan tidak lengkap. Seluruh penyebutan standar persyaratan keamanan berdasarkan Kebijakan Keamanan ini mengacu pada standar tertentu dan masing-masing versi penerusnya atau versi yang setara, sebagaimana dapat diperbarui, kecuali jika Amazon menentukan lain.