Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

KEBIJAKAN KEAMANAN VENDOR AMAZON

Terakhir diperbarui: 11 September 2024

1. **LINGKUP.** Pemasok akan mematuhi persyaratan keamanan ini ("Kebijakan Keamanan"). Kebijakan Keamanan ini tidak membatasi kewajiban kontraktual atau hukum Pemasok lainnya. Apabila terdapat perbedaan antara Kebijakan Keamanan ini dan perjanjian lain antara Pemasok dan Amazon, Pemasok akan mematuhi persyaratan yang lebih ketat yang lebih melindungi Informasi Amazon.

2. **PEMBARUAN.**

2.1 Amazon dapat melakukan pembaruan yang wajar secara komersial terhadap Kebijakan Keamanan ini dari waktu ke waktu, yang akan berlaku 30 hari setelah tanggal "Terakhir diperbarui" dari Kebijakan Keamanan ini. Pemasok setuju untuk terikat dengan Kebijakan Keamanan yang diperbarui setelah pembaruan berlaku.

2.2 Jika Pemasok ingin menerima pemberitahuan sebelumnya tentang pembaruan ini sebelum berlaku, Pemasok dapat berlangganan untuk menerima pemberitahuan pembaruan menggunakan formulir berlangganan yang disediakan di halaman web Kebijakan Keamanan ini. Pemasok akan memastikan bahwa semua informasi kontak Pemasok yang diberikan untuk langganan pemberitahuan pembaruan senantiasa terkini dan akurat. Pemasok akan dianggap telah menerima pemberitahuan pembaruan ketika dikirimkan melalui email, terlepas dari apakah Pemasok benar-benar menerima pemberitahuan pembaruan atau tidak.

3. **TUJUAN YANG DIIZINKAN.**

3.1 **Otorisasi Tegas**. Pemasok hanya dapat Memproses Informasi Amazon yang secara tegas diizinkan berdasarkan Perjanjian dan hanya untuk tujuan menyediakan produk atau layanan berdasarkan Perjanjian ("Tujuan yang Diizinkan").

3.2 **Penyimpanan Data**. Pemasok akan menyimpan Informasi Amazon hanya untuk tujuan dan selama diperlukan untuk Tujuan yang Diizinkan.

3.3 **Batasan Tegas**. Pemasok tidak akan: (a) Memproses Informasi Amazon apa pun, sekalipun Dianonimkan; (b) mengalihkan, menyewakan, menukar, memperdagangkan, menjual, meminjamkan, menyewagunakan, atau mendistribusikan atau menyediakan Informasi Amazon mana pun kepada pihak ketiga mana pun, sekalipun Dianonimkan; atau (c) mengembangkan, melatih, atau meningkatkan model Kecerdasan Buatan (Artificial Intelligence/AI) atau Pembelajaran Mesin (Machine Learning/ML) menggunakan Informasi Amazon, sekalipun Dianonimkan.

4. **PERSYARATAN KEAMANAN MINIMUM**. Pemasok akan memelihara pengamanan fisik, administratif, dan teknis yang konsisten dengan praktik terbaik industri (termasuk standar Organisasi Internasional untuk Standardisasi (International Organization for Standardization, "ISO") 27001 dan 27002, Kerangka Kerja Keamanan Siber Institut Nasional Standar dan Teknologi (National Institute of Standards and Technology, "NIST"), atau standar lainnya yang serupa). Perlindungan yang dipertahankan oleh Pemasok akan mencakup persyaratan minimum yang dijelaskan di bawah ini di Bagian 4.1 – 4.18.

4.1 **Program Keamanan Informasi Tertulis**. Pemasok akan memiliki program keamanan informasi tertulis yang: (a) mencakup kebijakan, prosedur, dan standar yang sesuai yang memenuhi persyaratan yang ditetapkan dalam Kebijakan Keamanan ini; (b) menunjuk titik kontak keamanan yang bertanggung jawab untuk menyampaikan dan mengelola masalah keamanan (termasuk Insiden Keamanan); (c) ditinjau sedikitnya setiap tahun dan diperbarui sebagaimana diperlukan; dan (d) berlaku untuk Personel. Pemasok akan memantau dan memberlakukan program keamanan informasi dan mengatasi pelanggaran.

Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

4.2 **Manajemen Patch**. Pemasok akan tetap memperbarui Sistem Informasi yang Dicakup dengan peningkatan, pembaruan, perbaikan bug, dan versi baru terkini. Pemasok akan menerapkan mitigasi untuk aset yang tidak dapat di-*patch*.

4.3 **Pencatatan**. Pemasok akan mengumpulkan, mengelola, dan menyimpan catatan audit, peristiwa, dan keamanan, termasuk: (a) data catatan tentang semua penggunaan (baik yang diizinkan maupun yang tidak diizinkan) akun atau kredensial Amazon yang diberikan kepada Pemasok untuk Tujuan yang Diizinkan, dan (b) data catatan tentang peniruan identitas, atau upaya peniruan identitas, personel atau Personel Amazon yang memiliki akses ke Informasi Amazon atau Sistem Informasi yang Dicakup. Catatan tersebut akan berisi data yang memadai untuk mengidentifikasi setiap peristiwa yang dicatat: (i) Personel atau akun yang memulai peristiwa, (ii) waktu peristiwa, dan (iii) sistem, data, atau sumber daya lain yang terdampak. Pemasok akan menganalisis log tersebut secara berkala untuk membantu mendeteksi, menyelidiki, dan memulihkan dari aktivitas yang tidak sah.

4.4 **Pertahanan Terhadap Malware**. Pemasok akan (a) menggunakan perangkat lunak antimalware atau kontrol keamanan yang setara untuk semua Sistem Informasi yang Dicakup; (b) menjaga pembaruan, tanda tangan, dan konfigurasi perangkat lunak antimalware atau kontrol keamanan yang setara; dan (c) mengonfigurasi sistem untuk mendeteksi, mencegah, dan memulihkan instalasi, penyebaran, dan pelaksanaan kode berbahaya atau tidak sah.

4.5 **Program Manajemen Risiko.** Pemasok akan memiliki program manajemen risiko keamanan informasi tertulis, yang menetapkan proses untuk analisis risiko, perlakuan risiko, penerimaan risiko, dan pengecualian.

4.6 **Pelatihan Kesadaran Keamanan**. Pemasok akan memberikan pelatihan tentang keamanan informasi dan privasi data kepada Personel setelah dipekerjakan dan sedikitnya setiap tahun setelahnya. Pemasok juga akan memastikan bahwa Personel diberi tahu secara tepat waktu tentang pembaruan kebijakan keamanan dan privasi data Pemasok.

4.7 **Inventaris Data**. Pemasok akan mendokumentasikan dan memelihara informasi terkait (a) Informasi Amazon yang Diprosesnya dan (b) bagaimana dan di mana Informasi Amazon tersebut Diproses (misalnya dalam diagram arsitektur terkini). Atas permintaan Amazon, Pemasok akan memberikan informasi ini kepada Amazon.

4.8 **Pengujian Keamanan.**

4.8.1 Pemasok akan melakukan pengujian tahunan untuk memastikan pihaknya memenuhi persyaratan Kebijakan Keamanan ini.

4.8.2 Pemasok akan melakukan pengujian penetrasi pertahanan keamanan Pemasok setidaknya setiap tahun. Pengujian penetrasi akan mencakup: (a) pengujian dari dalam dan luar jaringan Pemasok, (b) rekayasa sosial (misalnya, simulasi phishing), dan (c) pengujian keamanan untuk jaringan nirkabel. Pemasok akan mengatasi kerentanan yang diidentifikasi sebagai bagian dari program manajemen kerentanannya. Atas permintaan Amazon, Pemasok akan memberikan hasil pengujian penetrasi dan perbaikan kerentanan tersebut kepada Amazon.

4.9 **Keamanan Jaringan**. Pemasok akan melindungi Sistem Informasi yang Dicakup dengan membatasi akses jaringan tanpa izin, terutama dari jaringan eksternal. Pemasok akan memelihara dan mengonfigurasi firewall atau kontrol keamanan setara lainnya untuk melindungi sistem dari akses yang tidak sah dan akan meninjau rangkaian aturan firewall setidaknya setiap tahun untuk memastikan kasus bisnis yang valid dan terdokumentasi ada untuk semua aturan.

4.10 **Lingkungan yang Sesuai**. Pemasok hanya akan Memproses Informasi Amazon di lingkungan yang sesuai dengan tujuannya dan tidak akan Memproses Informasi Amazon di lingkungan pengujian, kecuali jika diizinkan berdasarkan Perjanjian.

4.11 **Enkripsi**. Pemasok akan mengenkripsi semua Informasi Amazon saat tidak digunakan dan dalam transit di seluruh jaringan eksternal sesuai dengan praktik terbaik industri. Jika Informasi Amazon ditransmisikan pada

jaringan Pemasok internal, informasi tersebut akan ditransmisikan melalui protokol terenkripsi yang memenuhi praktik terbaik industri. Pemasok akan mengelola dan mengamankan kunci enkripsi sesuai praktik terbaik industri.

4.12 **Penggunaan Hak Administratif yang Dikendalikan**. Pemasok akan mengelola fungsi administratif sesuai Kerangka Kerja Keamanan Siber NIST atau ISO 27002. Pemasok sedikitnya akan memisahkan akun administratif dari akun standar dan membatasi akun administratif agar hanya dapat memiliki kemampuan yang diperlukan untuk melaksanakan fungsi administratif. Pemasok akan mencatat semua tindakan akun administratif dengan cara yang dapat diatribusikan kepada pengguna individu. Kemampuan administratif yang diberikan ke akun standar akan berdasarkan hak istimewa terkecil dan dicatat dengan cara yang dapat diatribusikan kepada pengguna individu.

4.13 **Pengendalian Akses.**

4.13.1 **ID Unik**. Pemasok akan memberikan ID unik individu kepada Personel yang memiliki akses ke Informasi Amazon atau Sistem Informasi yang Dicakup, termasuk akun dengan akses administratif.

4.13.2 **Hanya yang "Perlu Tahu".** Pemasok akan membatasi akses ke Informasi Amazon dan Sistem Informasi yang Dicakup hanya kepada Personel yang "perlu tahu" untuk Tujuan yang Diizinkan.

4.13.3 **Peninjauan Akses Pengguna**. Pemasok akan, sedikitnya setiap 90 hari sekali, meninjau daftar Personel dan layanan yang memiliki akses ke Informasi Amazon dan Sistem Informasi yang Dicakup, serta menghapus akses dari akun yang tidak lagi memerlukannya.

4.13.4 **Single Sign-On (SSO)**. Setiap layanan Pemasok yang memerlukan autentikasi personel Amazon harus diintegrasikan dengan penyedia identitas Amazon (misalnya Amazon Federate) untuk menyediakan autentikasi tersebut. Layanan tersebut tidak boleh menggunakan kredensial yang disediakan Pemasok atau dikelola Pemasok untuk autentikasi.

4.14 **Manajemen Kata Sandi.**

4.14.1 **Kata Sandi yang Kuat**. Pemasok tidak akan menggunakan standar yang disediakan produsen untuk kata sandi sistem dan parameter keamanan lainnya pada Sistem Informasi yang Dicakup. Pemasok akan mewajibkan dan memastikan penggunaan "kata sandi yang kuat" yang diberlakukan sistem sesuai dengan praktik terbaik yang dijelaskan dalam NIST SP 800-63B pada semua Sistem Informasi yang Dicakup. Pemasok akan mewajibkan semua kata sandi dan kredensial akses dirahasiakan dan tidak dibagikan kepada Personel.

4.14.2 **Penguncian**. Pemasok akan mempertahankan dan memberlakukan "penguncian akun" dengan menonaktifkan akun yang memiliki akses ke Informasi Amazon atau Sistem Informasi yang Dicakup saat akun melampaui maksimal sepuluh (10) percobaan kata sandi yang salah secara berturut-turut.

4.15 **Akses Jarak Jauh; Autentikasi Multifaktor**. Pemasok akan menerapkan autentikasi multifaktor (yaitu memerlukan sedikitnya dua faktor untuk mengautentikasi pengguna) untuk akses jarak jauh ke jaringan, sistem, aplikasi, atau aset Pemasok lainnya.

4.16 **Akses "Massal"**. Untuk tujuan bagian ini, akses "massal" berarti mengakses data melalui kueri basis data, pembuatan laporan, atau transfer data massal lainnya.

4.16.1 Kecuali sebagaimana ditetapkan secara tegas dalam Perjanjian atau lainnya oleh Amazon secara tertulis, Pemasok tidak akan mengakses, dan tidak akan mengizinkan akses ke, Informasi Amazon "secara massal", terlepas dari apakah Informasi Amazon berada dalam basis data yang dikendalikan oleh Amazon atau Pemasok atau disimpan menggunakan metode lain, termasuk penyimpanan dalam arsip berbasis file (misalnya file flat).

4.16.2 Apabila Amazon mengizinkan akses "secara massal", Pemasok akan: (a) membatasi akses tersebut hanya untuk Personel tertentu yang "perlu tahu", dan (b) memerlukan otorisasi tegas dan pencatatan akses tersebut

Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

sesuai persyaratan Bagian 4.3. Berdasarkan permintaan Amazon
sesuai dengan Bagian 10 peninjauan keamanan atau Bagian 11 Insiden Keamanan, Pemasok akan memberikan kepada Amazon semua catatan akses “massal” yang disebutkan di bagian ini.

4.17 Pemisahan Data. Pemasok akan senantiasa memisahkan Informasi Amazon secara fisik atau logis dari informasi Pemasok dan pihak ketiga. Jika pemisahan tidak memungkinkan, Pemasok akan memastikan bahwa Informasi Amazon dapat dibedakan dari informasi lain untuk tujuan pencatatan, penghapusan, dan tanggapan insiden.

4.18 **Keamanan Personel Pemasok.**

4.18.1 Pemasok akan mengambil semua tindakan pencegahan yang wajar untuk memastikan bahwa Personel yang diberi akses ke Informasi Amazon akan menjaga kerahasiaannya dan menggunakannya hanya untuk Tujuan yang Diizinkan. Tindakan pencegahan ini harus mencakup pemberlakuan persyaratan kerahasiaan melalui perjanjian kerahasiaan atau kebijakan Pemasok.

4.18.2 Untuk setiap Personel yang (a) tidak lagi memerlukan akses ke Informasi Amazon atau (b) tidak lagi memenuhi syarat sebagai Personel Pemasok, Pemasok akan mengakhiri akses ke Informasi Amazon dan Sistem Informasi yang Dicakup dalam 24 jam. Jika Personel mana pun mempertahankan akses ke Informasi Amazon atau Sistem Informasi yang Dicakup lebih dari 24 jam setelah (a) atau (b) terjadi, Pemasok akan memberi tahu Amazon tentang akses berkelanjutan ini dalam 24 jam setelah Pemasok mengetahuinya dengan mengirimkan email ke security@amazon.com.

5. **PERSYARATAN KEAMANAN PEMBAYARAN**. Jika Pemasok memiliki akses ke atau akan Memproses data pemegang kartu pembayaran, Pemasok akan mematuhi versi terbaru Standar Keamanan Data Industri Kartu Pembayaran (Payment Card Industry Data Security Standard/PCI DSS).

6. **SUBKONTRAKTOR.**

6.1 Pemasok tidak akan melakukan subkontrak atau mendelegasikan kewajibannya berdasarkan Kebijakan Keamanan ini kepada pihak ketiga mana pun (secara bersama-sama disebut sebagai “Subkontraktor”) tanpa persetujuan tertulis sebelumnya dari Amazon. Tanpa mengabaikan keberadaan atau ketentuan subkontrak atau delegasi apa pun, Pemasok akan tetap bertanggung jawab atas pelaksanaan kewajibannya secara penuh berdasarkan Kebijakan Keamanan ini. Syarat dan ketentuan Kebijakan Keamanan ini akan mengikat Subkontraktor dan Personel Subkontraktor Pemasok.

6.2 Jika Pemasok menggunakan Sistem Informasi yang Dicakup Subkontraktor, Pemasok akan melakukan peninjauan keamanan Sistem Informasi yang Dicakup Subkontraktor dan pengendalian keamanannya, dan atas permintaan Amazon, akan memberikan kepada Amazon laporan berkala tentang pengendalian keamanan Sistem Informasi yang Dicakup Subkontraktor dalam format yang diminta oleh Amazon (misalnya Pernyataan Standar untuk Keterlibatan Pengesahan no. 16 (Standards for Attestation Engagement/SSAE 16)).

7. AKSES KE SISTEM INFORMASI YANG DIKELOLA AMAZON. Amazon dapat memberi Pemasok hak untuk Memproses Informasi Amazon melalui portal web atau situs web nonpublik atau ekstranet lainnya (masing-masing disebut “Sistem Informasi yang Dikelola Amazon”) hanya untuk Tujuan yang Diizinkan. Jika Amazon mengizinkan Pemasok untuk Memproses Informasi Amazon menggunakan Sistem Informasi yang Dikelola Amazon, Pemasok dan Personelnya harus mematuhi persyaratan berikut:

7.1 **Akun**. Pemasok akan memastikan bahwa Personel Pemasok hanya menggunakan akun(-akun) Sistem Informasi yang Dikelola Amazon yang ditetapkan Amazon untuk setiap individu dan akan mewajibkan Personel Pemasok untuk menjaga kerahasiaan kredensial akses mereka dan tidak membagikannya.

Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

7.2 **Sistem**. Pemasok dan Personelnya akan menggunakan Sistem Informasi yang Dikelola Amazon hanya melalui sistem atau aplikasi komputasi atau pemrosesan (a) menjalankan sistem operasi yang dikelola oleh Pemasok dan yang menggunakan enkripsi disk penuh, dan (b) memenuhi persyaratan Bagian 4.2 (Manajemen patch), 4.4 (Pertahanan terhadap malware), dan 4.9 (Keamanan jaringan).

7.3 **Pembatasan**. Kecuali jika disetujui sebelumnya secara tertulis oleh Amazon, Pemasok dan Personelnya tidak akan mengunduh, meniru, atau menyimpan secara permanen Informasi Amazon apa pun dari Sistem Informasi yang Dikelola Amazon di media apa pun.

7.4 **Pengakhiran Akun**. Untuk setiap Personel yang (a) tidak lagi memerlukan akses ke Sistem Informasi yang Dikelola Amazon atau (b) tidak lagi memenuhi syarat sebagai Personel Pemasok (misalnya individu yang keluar dari pekerjaan Pemasok), Pemasok akan segera menghentikan akses Personel tersebut (dalam waktu maksimum 24 jam) ke Sistem Informasi yang Dikelola Amazon atau memberi tahu Amazon untuk menghapus akses tersebut.

8. **DOMAIN ATAU URL AMAZON.** Setiap domain atau URL yang disediakan Pemasok untuk penggunaan Amazon sendiri tidak boleh diterbitkan oleh Pemasok untuk atau digunakan kembali oleh pihak ketiga mana pun selama sedikitnya 5 tahun setelah pengakhiran Perjanjian.

9. PENGEMBALIAN DAN PENGHAPUSAN DATA; PEMUSNAHAN FORENSIK MEDIA.

9.1 **Pengembalian dan Penghapusan Data**. Atas permintaan Amazon, Pemasok akan segera (tetapi tidak lebih dari 72 jam) mengembalikan kepada Amazon dan secara permanen dan aman menghapus semua Informasi Amazon sesuai pemberitahuan Amazon yang mewajibkan pengembalian dan/atau penghapusan. Pemasok juga akan secara permanen dan aman menghapus semua instans Informasi Amazon secara langsung (online atau dapat diakses jaringan) dalam waktu 30 hari setelah penyelesaian Tujuan yang Diizinkan atau pengakhiran atau berakhirnya Perjanjian. Jika diminta oleh Amazon, Pemasok akan menyatakan secara tertulis bahwa semua Informasi Amazon telah dihapus. Agar jelas, bagian ini tidak akan berlaku untuk Salinan Arsip sesuai Bagian 9.3.

9.2 **Sanitasi Data**. Semua Informasi Amazon yang dihapus oleh Pemasok akan dihapus sesuai dengan Rekomendasi Sanitasi Minimum yang tercantum dalam NIST SP 800-88 Revisi 1, Pedoman Sanitasi Media (18 Desember 2014, Apendiks A) untuk pembersihan jenis perangkat terkait. Jika tidak ada pedoman dalam NIST SP 800-88 untuk jenis perangkat yang relevan, Pemasok akan memusnahkan perangkat yang berisi Informasi Amazon dengan salah satu cara berikut: (a) membersihkan sebagaimana didefinisikan dalam NIST SP 800-88, (b) memusnahkan sebagaimana ditetapkan dalam NIST SP 800-88, atau (c) melalui standar lain yang mungkin diperlukan Amazon berdasarkan klasifikasi dan sensitivitas Informasi Amazon.

9.3 **Salinan Arsip**. Jika Pemasok diwajibkan oleh hukum untuk menyimpan salinan arsip Informasi Amazon, Pemasok tidak akan menggunakan Informasi Amazon yang diarsipkan untuk tujuan lain dan akan tetap terikat dengan semua kewajibannya berdasarkan Kebijakan Keamanan ini. Setiap Informasi Amazon yang diarsipkan harus dienkripsi dan disimpan jika Sistem Informasi yang Dicakup yang meng-*host* atau menyimpan Informasi Amazon yang dienkripsi tidak memiliki akses ke salinan kunci(-kunci) yang digunakan untuk enkripsi. Setiap pencadangan offline atau “dingin” (yaitu tidak tersedia untuk penggunaan langsung atau interaktif) harus disimpan di fasilitas yang aman secara fisik.

9.4 **Pemusnahan Forensik Media**. Sebelum membuang perangkat keras, perangkat lunak, atau media lain yang berisi atau sewaktu-waktu berisi Informasi Amazon, Pemasok akan melakukan pemusnahan forensik lengkap terhadap perangkat keras, perangkat lunak, atau media lain sesuai NIST SP 800-88, Apendiks A. Persyaratan pemusnahan ini tidak akan berlaku untuk media penyimpanan yang tidak memiliki akses atau kendali fisik terhadap Pemasok. Dalam kasus tersebut, Pemasok akan memastikan bahwa Informasi Amazon dihapus dengan aman saat tidak lagi diperlukan sesuai praktik terbaik industri.

Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

9.4.1 Kecuali Pemasok menerima persetujuan tertulis sebelumnya secara tegas dari Amazon, Pemasok tidak akan menjual, menjual kembali, menyumbangkan, memperbarui, atau mentransfer perangkat keras, perangkat lunak, atau media lain yang sewaktu-waktu berisi Informasi Amazon kecuali jika telah
dimusnahkan secara forensik sesuai Bagian ini.

10. **TINJAUAN KEAMANAN**. Atas permintaan Amazon, Pemasok akan: (a) menyelesaikan penilaian risiko Amazon, (b) memberikan bukti yang diminta oleh Amazon untuk memvalidasi kepatuhan Pemasok terhadap Kebijakan Keamanan ini, (c) mengizinkan Amazon atau pihak ketiga yang ditunjuk atas namanya untuk melakukan peninjauan kepatuhan Pemasok terhadap Kebijakan Keamanan ini, dan/atau (d) memberikan kepada Amazon semua catatan yang disebutkan di Bagian 4.3 dalam format Kerangka Kerja Skema Keamanan Siber Terbuka (Open Cybersecurity Schema Framework/OCSF). Jika Pemasok mewajibkan bahwa bukti apa pun ditinjau secara langsung atau dalam inspeksi di lokasi, bukannya memberikan bukti tersebut untuk ditinjau Amazon dari jarak jauh, Pemasok akan menanggung biaya perjalanan dan pengeluaran lain terkait inspeksi di lokasi tersebut. Jika penilaian atau peninjauan mengidentifikasi temuan, atas biaya dan pengeluaran Pemasok sendiri, Pemasok akan segera mengambil semua tindakan wajar yang diperlukan untuk memulihkan temuan tersebut demi kepuasan wajar Amazon dan dalam jangka waktu yang disepakati.

11. **INSIDEN KEAMANAN.**

11.1 **Pemberitahuan Insiden Keamanan**. Pemasok akan memberi tahu Amazon sesegera mungkin, namun tidak lebih dari 24 jam setelah Pemasok mengetahui atau meyakini secara wajar bahwa telah terjadi akses, pengumpulan, akuisisi, penggunaan, transmisi, pengungkapan, kerusakan, atau kehilangan Informasi Amazon atau Sistem Informasi yang Dicakup tanpa izin (“Insiden Keamanan”). Pemasok akan mengirimkan pemberitahuan Insiden Keamanan ke security@amazon.com.

11.2 **Rencana Tanggapan Insiden**. Pemasok akan memiliki rencana tanggapan insiden tertulis dan memberikan salinannya kepada Amazon jika diminta. Pemasok akan memperbaiki setiap Insiden Keamanan secara tepat waktu sesuai rencana tanggapan insiden tertulis Pemasok dan praktik terbaik industri. Pemasok akan meninjau, menguji, dan (jika diperlukan) memperbarui rencana sedikitnya setiap tahun.

11.3 **Kerja Sama dengan Amazon**. Pemasok akan (a) membantu penyelidikan Amazon atas Insiden Keamanan; (b) memfasilitasi wawancara dengan Personel dan pihak lain yang terlibat dalam Insiden atau tanggap keamanan; (c) menyimpan perincian tertulis tentang penyelidikan dan tanggapan Insiden Keamanan Pemasok; dan (d) menyediakan kepada Amazon semua catatan, log, file, pelaporan data, laporan forensik, laporan penyelidikan, dan materi lain yang diminta oleh Amazon.

11.4 **Pemberitahuan Pihak Ketiga**. Kecuali jika diwajibkan lain oleh hukum, Pemasok akan memperoleh persetujuan tertulis sebelumnya dari Amazon sebelum: (a) memberi tahu pihak ketiga (termasuk otoritas regulasi atau pelanggan) tentang Insiden Keamanan apa pun; atau (b) mengidentifikasi Amazon dalam pemberitahuan atau pernyataan publik apa pun terkait Insiden Keamanan apa pun. Kecuali jika diwajibkan lain oleh hukum, Amazon akan berhak untuk menentukan jika pemberitahuan Insiden Keamanan akan diberikan kepada pihak ketiga mana pun serta bentuk, waktu, dan konten pemberitahuan tersebut.

12. **PEMBERITAHUAN PROSES HUKUM**. Pemberitahuan proses hukum. Kecuali jika dilarang oleh hukum, jika Informasi Amazon diminta untuk menanggapi proses hukum atau hukum lain yang berlaku, Pemasok akan memberikan pemberitahuan yang memadai kepada Amazon agar Amazon dapat meminta perintah perlindungan atau pemulihan lain yang sesuai.

13. **DEFINISI**.

13.1 “**Perjanjian**” berarti setiap perjanjian yang merujuk pada Kebijakan Keamanan ini.

Terjemahan di bawah hanya disediakan untuk tujuan informasi. Apabila terdapat perbedaan, ketidaksesuaian, atau pertentangan antara terjemahan ini dan versi bahasa Inggris yang telah diperbarui terakhir kali (termasuk karena penundaan terjemahan), versi bahasa Inggris akan berlaku.

13.2 “**Amazon**” berarti Amazon.com, Inc. dan afiliasinya.

13.3 “**Informasi Amazon**” berarti: (a) semua Informasi Rahasia Amazon (sebagaimana didefinisikan dalam perjanjian lain antara para pihak); (b) semua data, catatan, file, konten, atau informasi, dalam bentuk apa pun, diperoleh, diakses, dikumpulkan, diterima, disimpan, atau dikelola oleh Pemasok atau afiliasinya, dari atau atas nama Amazon, atau sehubungan dengan Perjanjian; dan (c) informasi yang berasal dari (a) atau (b), bahkan jika Dianonimkan.

13.4 “**Menganonimkan**” berarti Memproses data atau informasi apa pun (termasuk Informasi Amazon) dengan cara atau bentuk yang tidak mengidentifikasi, mengizinkan identifikasi, dan tidak diatribusikan kepada Amazon, atau pengguna, pengidentifikasi perangkat, sumber, produk, layanan, konteks, atau merek apa pun daripadanya.

13.5 “**Sistem Informasi yang Dicakup**” berarti setiap sistem yang digunakan Pemasok untuk Memproses Informasi Amazon.

13.6 “**Personel**” berarti karyawan Pemasok atau Subkontraktor, agen, Subkontraktor, dan pengguna resmi lainnya dari sistem dan sumber daya jaringannya.

13.7 “**Proses**” berarti melakukan operasi apa pun pada data, seperti akses, penggunaan, pengumpulan, penerimaan, penyimpanan, perubahan, transmisi, penyebaran, atau penyediaan, penghapusan, atau pemusnahan.

13.8 “**Pemasok**” berarti setiap pemasok, vendor, atau kontraktor yang ditetapkan dalam Perjanjian dan penyedia lain yang tunduk pada Perjanjian.