RINGKASAN LANGKAH-LANGKAH KEAMANAN HP

Untuk melindungi data Pelanggan, HP mematuhi serangkaian kontrol keamanan informasi yang kuat, termasuk kebijakan, praktik, prosedur, dan struktur organisasi untuk menjaga kerahasiaan, integritas, dan ketersediaan informasinya sendiri dan informasi pelanggannya (termasuk Data Pribadi sebagaimana ditetapkan dalam Adendum Pelanggan dan Pemrosesan Data HP). Berikut adalah ikhtisar tindakan keamanan teknis/organisasi di seluruh perusahaan HP.

1. Kebijakan Keamanan

   HP menerapkan kebijakan, standar, dan prosedur yang berlaku secara global yang ditujukan untuk melindungi data HP dan Pelanggan. Detail kebijakan keamanan HP bersifat rahasia untuk melindungi integritas data dan sistem HP. Namun, berikut ringkasan kebijakan-kebijakan utama kami.

2. Organisasi Keamanan Informasi

   Program Keamanan Informasi HP dirancang untuk mengarahkan dan menjalankan strategi dan kontrol keamanan informasi organisasi. Sistem ini memastikan seluruh perusahaan mematuhi kebijakan dan kontrol keamanan HP, serta mematuhi persyaratan keamanan pelanggannya. Disusun sesuai dengan kerangka kerja, hukum, dan peraturan keamanan siber tingkat industri, Kerangka Kerja ini ditinjau setiap tahun untuk disesuaikan dengan lanskap ancaman yang terus berkembang di HP.

3. Manajemen Risiko Keamanan Siber

   Program manajemen risiko keamanan siber HP dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan aset informasinya. Program ini menyediakan pendekatan yang konsisten untuk mengidentifikasi, menilai, memprioritaskan, menangani, memperbaiki, melacak, dan melaporkan risiko keamanan siber. HP mendefinisikan Penerima Risiko sebagai tingkat kerugian yang dapat diterima dan Toleransi Risiko sebagai tingkat variasi dari penerimaan ini. Risiko dievaluasi menggunakan metodologi yang telah ditetapkan, sehingga HP dapat mengurangi risiko keamanan informasi hingga ke tingkat yang dapat diterima. Program ini selaras dengan proses Manajemen Risiko Perusahaan di HP.

4. Keamanan SDM

   Kebijakan Keamanan Sumber Daya Manusia HP memastikan keamanan informasi di seluruh siklus hidup karyawan dengan menetapkan proses untuk mengakses fasilitas, sistem informasi, dan aset lainnya. Hal ini termasuk mendapatkan pengakuan tertulis melalui perjanjian kerahasiaan dan larangan pengungkapan, serta melakukan prosedur pemeriksaan latar belakang. Semua calon karyawan HP harus menyelesaikan pemeriksaan verifikasi latar belakang sesuai dengan hukum, peraturan, dan kode etik yang berlaku.

5. Manajemen Aset

   HP memiliki proses untuk mengidentifikasi aset informasi teknis, mengategorikan aset penting, dan menerapkan prosedur penanganan yang terdokumentasi untuk setiap jenis klasifikasi informasi, termasuk yang berisi Data Pribadi. Prosedur ini mencakup penyimpanan, pengalihan, penyampaian, akses, pencatatan, penyimpanan, pemusnahan, pembuangan, manajemen insiden, dan pemberitahuan adanya pelanggaran. Kebijakan dan standar keamanan HP juga mewajibkan pembuangan media secara aman.

6. Keamanan Data

   Program Keamanan Data HP menguraikan praktik keamanan dan kontrol teknis yang harus diterapkan untuk melindungi kerahasiaan, keaslian, dan integritas data. Persyaratan hukum, nilai, tingkat kepentingan, dan kepekaan terhadap pengungkapan atau modifikasi yang tidak sah adalah beberapa faktor yang menentukan klasifikasi informasi berdasarkan kebijakan Keamanan Data HP. Selain prosedur penanganan data, kebijakan ini juga menjelaskan tentang enkripsi data, penghapusan, pengumpulan dan pemrosesan, penyimpanan, pencadangan, dan pencegahan kehilangan data.

7. Kontrol Akses

   HP menggunakan prinsip hak istimewa paling sedikit untuk kontrol akses logis, menyediakan akses pengguna melalui ID pengguna dan kata sandi yang berbeda-beda. Kebijakan kata sandi menentukan kompleksitas, kekuatan, validitas, dan kontrol riwayat kata sandi. Hak akses ditinjau secara berkala dan dicabut saat karyawan keluar dari perusahaan. Prosedur yang disepakati untuk pembuatan dan penghapusan akun pengguna diimplementasikan untuk memberikan dan mencabut akses ke sistem klien selama penugasan.

8. Kriptografi

   HP telah menetapkan serangkaian proses kriptografi yang andal untuk memastikan kerahasiaan, integritas, dan ketersediaan aset informasi. Protokol yang disetujui memerlukan enkripsi untuk aset tertentu, termasuk aset yang berisi data pribadi. Program Kriptografi kami menggunakan teknik matematika untuk mengamankan informasi dan komunikasi, memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang. Komponen penting di dalam program keamanan informasi HP adalah melindungi data dari akses yang tidak sah dan kerusakan.

9. Keamanan Fisik dan Lingkungan

   Fasilitas HP diamankan menggunakan berbagai kontrol akses fisik dan elektronik, termasuk petugas keamanan, kontrol akses elektronik, dan kamera pengawas (CCTV). Fasilitas juga dilengkapi dengan dukungan infrastruktur yang diperlukan, termasuk pengatur suhu dan cadangan daya, menggunakan UPS dan/atau generator diesel untuk mendukung layanan-layanan penting. Semua personel HP telah terdaftar dan diwajibkan membawa tanda pengenal yang sesuai.

10. Manajemen Operasi

    HP telah menetapkan persyaratan penguatan minimum untuk infrastruktur teknologi, termasuk tempat kerja, server, dan peralatan jaringan. Perangkat ini menggunakan gambar sistem operasi yang sudah diperkuat sebelumnya, dengan persyaratan yang berbeda-beda sesuai dengan sistem operasi dan kontrol yang diterapkan. Selain itu, HP telah menerapkan Sistem Deteksi/Pencegahan Penyusupan Jaringan (NIDS/NIPS) yang dipantau dan dikelola 24/7.

11. Keamanan Komunikasi

    Keamanan Komunikasi memastikan perlindungan informasi dalam jaringan perusahaan. Di dalamnya termasuk instalasi dan pengelolaan komponen keamanan jaringan (misalnya, firewall), pemisahan jaringan, serta pemfilteran web dan kontrol penanganan email. Selain itu, ada pula pemantauan dan pengelolaan saluran komunikasi untuk mendeteksi dan mencegah akses yang tidak sah atau pembobolan data.

12. Keamanan Sistem

    Kebijakan HP mengharuskan penggunaan metodologi pengembangan yang aman untuk sistem dan perangkat lunak di sepanjang siklus hidupnya. Siklus Hidup Pengembangan Perangkat Lunak mencakup inisiasi, pengembangan/akuisisi, implementasi, operasi, dan pembuangan. Semua komponen sistem dievaluasi untuk mengetahui dampaknya terhadap keamanan secara keseluruhan. HP telah menetapkan kontrol untuk transaksi layanan aplikasi, termasuk validasi kredensial pengguna, tanda tangan digital, enkripsi, protokol komunikasi yang aman, dan menyimpan detail transaksi dalam zona keamanan jaringan yang sesuai. Selain itu juga dilakukan pemindaian kerentanan internal secara rutin.

13. Pihak Ketiga dan Subkontraktor

    HP memiliki proses untuk memilih subkontraktor yang memenuhi persyaratan keamanan kontrak yang komprehensif. Untuk pemasok tertentu yang menangani data HP atau pelanggan, atau mengakses jaringan HP, Keamanan Siber HP melakukan penilaian risiko untuk memverifikasi program keamanan informasi dengan perlindungan fisik, teknis, dan administratif. Penilaian ini diperlukan sebelum pemasok mengakses informasi HP.

14. Manajemen Insiden Keamanan Informasi

    HP memiliki Proses Manajemen Insiden Siber yang komprehensif yang menguraikan tujuan, ruang lingkup, peran, tanggung jawab, komitmen manajemen, koordinasi organisasi, prosedur implementasi, dan pemeriksaan kepatuhan. Proses ini ditinjau dan diperbarui setiap tahun. Tim Penanganan Insiden Siber, termasuk personel Keamanan Siber HP yang terlatih dalam penanganan insiden dan manajemen krisis, meninjau proses dan setiap insiden atau kejadian secara rutin.

15. Manajemen Kelangsungan Bisnis

    Program Kelangsungan Operasi global HP memastikan kelangsungan menyeluruh melalui proses perencanaan yang kolaboratif, terstandarkan, dan terdokumentasi. Perusahaan secara berkala menjalankan rencana kelangsungan bisnisnya untuk memastikan efektivitas, menguji dan memperbarui semua rencana setidaknya setiap tahun. Selain itu, semua personel yang terlibat dalam rencana kelangsungan bisnis mendapatkan pelatihan yang tepat.

16. Kepatuhan

    Kepatuhan membentuk pendekatan HP dalam memenuhi persyaratan hukum, kontrak, dan persyaratan internal untuk program keamanan informasi yang efektif. Tinjauan keamanan informasi secara berkala memastikan adanya integrasi protokol ke dalam setiap operasi kelompok bisnis. Proses peninjauan juga memastikan bahwa dokumen-dokumen yang ada selalu diperbarui untuk merefleksikan kewajiban hukum yang berlaku saat ini sesuai perubahan persyaratan.

17. Industri Kartu Pembayaran

    Kerangka kerja Industri Kartu Pembayaran (PCI) menjadi acuan pendekatan HP dalam mencapai Kepatuhan PCI, yang menjelaskan tanggung jawab bisnis dan kontrol keamanan yang selaras dengan PCI DSS. Dengan menginstal dan menggunakan kontrol keamanan jaringan seperti firewall, HP dipastikan memenuhi persyaratan Kepatuhan PCI.

18. Keamanan Produk HP

    Keamanan Produk HP mencakup praktik-praktik penting dalam menjaga keamanan Produk HP, seperti penandatanganan kode, pengelolaan kerentanan keamanan produk, penerbitan buletin keamanan, dan pelaporan masalah keamanan produk. Langkah-langkah ini memastikan bahwa produk HP tetap aman dan dapat diandalkan oleh pengguna. Keamanan produk sangat penting bagi HP karena dapat membantu mempertahankan kepercayaan pelanggan dan melindungi mereka dari potensi ancaman.

19. Keamanan Layanan HP

    Keamanan Layanan HP mencakup praktik-praktik penting dalam menjaga keamanan layanan yang diberikan kepada pelanggan HP. Kebijakan ini mencakup berbagai bidang keamanan layanan, termasuk lingkungan yang di-host infrastruktur HP, yang di-host pihak ketiga, yang di-host mitra, dan yang di-host pelanggan. Langkah-langkah ini memastikan bahwa layanan HP tetap aman dan dapat diandalkan oleh pengguna. Dengan menerapkan praktik keamanan yang kuat, HP memastikan keamanan dan integritas produk dan layanannya, sehingga menciptakan lingkungan yang aman dan dapat dipercaya bagi semua pengguna.