ZHRNUTIE BEZPEČNOSTNÝCH OPATRENÍ SPOLOČNOSTI HP

Na ochranu údajov Zákazníka spoločnosť HP dodržiava rozsiahlu súpravu kontrol zabezpečenia informácií vrátane zásad, praktík, postupov a organizačných štruktúr s cieľom zachovať dôvernosť, integritu a dostupnosť svojich vlastných informácií a informácií svojich zákazníkov (vrátane osobných údajov, ktoré sú definované v dodatku spoločnosti HP pre zákazníka a spracovanie údajov). V nasledujúcom texte je uvedený prehľad technických/organizačných bezpečnostných opatrení spoločnosti HP v celej spoločnosti.

1. Bezpečnostné zásady

   Spoločnosť HP udržiava celosvetovo platné zásady, normy a postupy určené na ochranu údajov spoločnosti HP a Zákazníka. Podrobnosti bezpečnostných zásad spoločnosti HP sú dôverné, aby sa chránila integrita údajov a systémov spoločnosti HP. Zhrnutie našich kľúčových zásad však nájdete nižšie.

2. Organizácia zabezpečenia informácií

   Program zabezpečenia informácií spoločnosti HP je navrhnutý tak, aby riadil a udržiaval stratégiu a kontroly zabezpečenia informácií organizácie. Tento systém zabezpečuje celopodnikový súlad s bezpečnostnými zásadami a kontrolami spoločnosti HP, ako aj dodržiavanie bezpečnostných požiadaviek svojich zákazníkov. Rámec, štruktúrovaný v súlade s priemyselnými normami kybernetickej bezpečnosti, zákonmi a nariadeniami, sa každoročne skúma, aby sa prispôsobil vyvíjajúcemu sa prostrediu hrozieb spoločnosti HP.

3. Riadenie kybernetickej bezpečnosti

   Program spoločnosti HP pre riadenie kybernetickej bezpečnosti je navrhnutý tak, aby chránil zachovanie dôvernosti, integrity a dostupnosti svojich informačných aktív. Program poskytuje konzistentný prístup k identifikácii, posúdeniu, stanoveniu priorít, liečbe, náprave, sledovaniu a podávaniu správ o kybernetických bezpečnostných rizikách. Spoločnosť HP definuje svoju chuť k riziku ako prijateľnú úroveň vystavenia sa strate a toleranciu voči riziku ako stupeň odchýlky od tejto chuti. Riziká sa hodnotia pomocou definovanej metodiky, čo umožňuje spoločnosti HP zmierniť riziká v oblasti zabezpečenia informácií na prijateľnú úroveň. Tento program je v súlade s procesom riadenia podnikových rizík spoločnosti HP.

4. Bezpečnosť v oblasti HR

   Zásady spoločnosti HP v oblasti ľudských zdrojov zaisťuje zabezpečenie informácií počas celého životného cyklu zamestnancov zriaďovaním procesov prístupu k zariadeniam, informačným systémom a iným aktívam. To zahŕňa získanie písomných potvrdení prostredníctvom dohôd o dôvernosti a o mlčanlivosti, ako aj vykonávanie postupov preverovania. Všetci kandidáti na zamestnanie v spoločnosti HP musia dokončiť previerku v súlade s príslušnými zákonmi, právnymi predpismi a etikou.

5. Správa aktív

   Spoločnosť HP má k dispozícii proces identifikácie aktív technických informácií, kategorizácie kritických aktív a údržby zdokumentovaných postupov manipulácie pre každý typ klasifikácie informácií vrátane tých, ktoré obsahujú osobné údaje. Tieto postupy sa týkajú skladovania, prenosu, komunikácie, prístupu, prihlasovania, zadržania, zničenia, likvidácie, riadenia incidentov a oznámenia o porušení. Bezpečnostné zásady a normy spoločnosti HP tiež prikazujú bezpečnú likvidáciu médií.

6. Zabezpečenie údajov

   Program zabezpečenia údajov spoločnosti HP vysvetľuje bezpečnostné postupy a technické kontroly, ktoré musia byť zavedené s cieľom chrániť dôvernosť, pravosť a integritu údajov. Právne požiadavky, hodnota, kritickosť a citlivosť na neoprávnené zverejnenie alebo úpravy sú niektoré z faktorov, ktoré určujú, ako sú informácie klasifikované podľa zásad zabezpečenia údajov spoločnosti HP. Okrem postupov manipulácie s údajmi sa v zásadách opisuje šifrovanie údajov, odstraňovanie, zber a spracovanie, uchovanie, zálohovanie a prevencia pred stratou údajov.

7. Ovládanie prístupu

   Spoločnosť HP uplatňuje princíp najmenších privilégií na kontrolu logického prístupu a poskytuje prístup používateľa prostredníctvom jedinečných používateľských identifikátorov a hesiel. Zásady hesla definujú zložitosť, silu, platnosť a ovládacie prvky histórie hesiel. Prístupové práva sa pri odchode personálu pravidelne prehodnocujú a rušia. Na udelenie a zrušenie prístupu do klientskych systémov počas zapojenia sú implementované dohodnuté postupy na vytvorenie a vymazanie používateľského účtu.

8. Šifrovanie

   Spoločnosť HP definuje súbor širokých procesov šifrovania, aby zabezpečila dôvernosť, integritu a dostupnosť informačných aktív. Schválené protokoly vyžadujú šifrovanie pre určité aktíva vrátane aktív, ktoré obsahujú osobné údaje. Náš program šifrovania zahŕňa použitie matematických techník na zabezpečenie informácií a komunikácie, čím sa zaistí, aby k údajom mohli pristupovať len oprávnené strany. Kľúčovou zložkou programu zabezpečenia informácií spoločnosti HP je ochrana údajov pred neoprávneným prístupom a manipuláciou.

9. Fyzická a environmentálna bezpečnosť

   Zariadenia spoločnosti HP sú zabezpečené pomocou rôznych fyzických a elektronických kontrol prístupu vrátane bezpečnostných strážcov, elektronickej kontroly prístupu a uzavretého televízneho okruhu (CCTV). Zariadenia sú tiež vybavené potrebnou podporou infraštruktúry vrátane kontroly teploty a zálohovania energie pomocou UPS a/alebo naftových generátorov na podporu kritických služieb. Všetok personál spoločnosti HP je registrovaný a musí mať pri sebe príslušné identifikačné odznaky.

10. Prevádzkové riadenie

    Spoločnosť HP zaviedla minimálne požiadavky na spevnenie pre technologickú infraštruktúru vrátane pracovných staníc, serverov a sieťových zariadení. Tieto zariadenia používajú vopred spevnené obrázky operačného systému, pričom požiadavky sa líšia podľa operačného systému a implementovaných ovládacích prvkov. Okrem toho nasadila spoločnosť HP sieťové systémy detekcie/prevencie vniknutia (NIDS/NIPS), ktoré sú monitorované a spravované dvadsaťštyri hodín denne.

11. Bezpečnosť komunikácií

    Bezpečnosť komunikácií zabezpečuje ochranu informácií v rámci podnikových sietí. Patrí sem inštalácia a riadenie súčastí sieťovej bezpečnosti (napr. brány firewall), segregácia sietí, ako aj kontroly filtrovania webu a manipulácie s e-mailami. Okrem toho zahŕňa monitorovanie a správu komunikačných kanálov s cieľom odhaliť a zabrániť neoprávnenému prístupu alebo porušeniu údajov.

12. Zabezpečenie systémov

    Zásady spoločnosti HP riadia metodiku bezpečného vývoja systémov a softvéru počas celého ich životného cyklu. Životný cyklus vývoja softvéru zahŕňa iniciovanie, vývoj/akvizíciu, implementáciu, prevádzku a likvidáciu. Všetky systémové súčasti sa hodnotia na základe ich dopadu na celkové zabezpečenie. Spoločnosť HP zaviedla kontroly pre transakcie služieb aplikácií vrátane overenia prístupových údajov používateľa, digitálnych podpisov, šifrovania, protokolov zabezpečenej komunikácie a ukladania detailov transakcie v rámci príslušnej zóny zabezpečenia siete. Taktiež sa vykonáva pravidelné skenovania vnútorných slabých miest.

13. Tretie strany a subdodávatelia

    Spoločnosť HP má postupy výberu subdodávateľov, ktorí dodržiavajú komplexné zmluvné požiadavky zabezpečenia. V prípade príslušných dodávateľov, ktorí manipulujú s údajmi spoločnosti HP alebo zákazníkov, alebo majú prístup k sieti HP, spoločnosť HP Cybersecurity vykonáva hodnotenie rizík na overenie programu zabezpečenia informácií s fyzickými, technickými a administratívnymi zárukami. Toto hodnotenie je povinné predtým, ako môže dodávateľ získať prístup k informáciám od spoločnosti HP.

14. Riadenie incidentov zabezpečenia informácií

    Spoločnosť HP má komplexný proces riadenia kybernetických incidentov, ktorý načrtáva účel, rozsah, úlohy, povinnosti, záväzok riadenia, organizačnú koordináciu, vykonávacie postupy a kontrolu súladu. Tento proces sa ročne skúma a aktualizuje. Tím reakcie na kybernetické incidenty vrátane personálu spoločnosti HP vyškoleného v oblasti reakcie na incidenty a riadenia krízy vykonáva pravidelné kontroly procesu a akýchkoľvek incidentov alebo udalostí.

15. Riadenie kontinuity činností

    Globálny program kontinuity prevádzky spoločnosti HP zabezpečuje kontinuitu činností prostredníctvom spoločného, štandardizovaného a zdokumentovaného plánovania. Spoločnosť pravidelne vykonáva svoje plány na zabezpečenie kontinuity činností s cieľom zabezpečiť efektívnosť, testovanie a aktualizáciu všetkých plánov aspoň raz za rok. Všetci pracovníci zapojení do plánu kontinuity činností majú navyše riadne školenie.

16. Súlad s pravidlami

    Súlas s pravidlami formuje prístup spoločnosti HP k plneniu právnych, zmluvných a interných očakávaní v súvislosti s účinným programom zabezpečenia informácií. Pravidelné hodnotenia zabezpečenia informácií zaisťujú, že protokoly sú integrované do prevádzky každej obchodnej skupiny. Proces hodnotenia tiež udržiava dokumenty aktualizované tak, aby zohľadňovali súčasné právne záväzky vzhľadom na vývoj požiadaviek.

17. Odvetvie platobných kariet

    Rámec odvetvia platobných kariet (PCI) slúži ako sprievodca prístupom spoločnosti HP k dosiahnutiu súladu s rámcom PCI, pričom uvádza obchodné povinnosti a bezpečnostné kontroly zosúladené s rámcom PCI DSS. Spoločnosť HP inštaláciou a údržbou bezpečnostných kontrol, ako sú brány firewall, zabezpečí, že bude v súlade s rámcom PCI.

18. Zabezpečenie produktov HP

    Zabezpečenie produktov HP zahŕňa základné postupy na zabezpečenie produktov spoločnosti HP, ako napríklad podpisovanie kódu, riadenie slabých miest zabezpečenia produktu, vydanie bulletinov o zabezpečení a hlásenie bezpečnostných problémov produktu. Tieto opatrenia zabezpečujú, aby produkty spoločnosti HP zostali pre používateľov bezpečné a spoľahlivé. Zabezpečenie produktov je v spoločnosti HP prvoradé, pretože pomáha zachovať dôveru zákazníkov a chráni ich pred potenciálnymi hrozbami.

19. Zabezpečenie služieb HP

    Zabezpečenie služieb HP zahŕňa základné postupy na zabezpečenie služieb poskytovaných zákazníkom spoločnosti HP. Tieto zásady sa zaoberajú rôznymi oblasťami zabezpečenia služieb vrátane hostiteľskej infraštruktúry HP, hostiteľského prostredia tretích strán, hostiteľského partnera a prostredia, v ktorom je zákazník hostiteľom. Tieto opatrenia zaisťujú, aby služby spoločnosti HP zostali pre používateľov bezpečné a spoľahlivé. Implementovaním širokých bezpečnostných postupov spoločnosť HP zabezpečuje bezpečnosť a integritu svojich produktov a služieb a podporuje bezpečné a dôveryhodné prostredie pre všetkých používateľov.