SAŽETAK SIGURNOSNIH MJERA TVRTKE HP

Kako bi zaštitio podatke klijenata, HP se pridržava snažnog skupa kontrola za zaštitu podataka uključujući pravila, prakse, postupke i organizacijske strukture kako bi zaštitio povjerljivost, integritet i dostupnost svojih podataka i podataka klijenata (uključujući osobne podatke kako je definirano u Dodatku o obradi klijenata i podataka tvrtke HP). U nastavku slijedi pregled tehničkih/organizacijskih sigurnosnih mjera tvrtke HP koje se provode u cijeloj tvrtki.

1. Sigurnosna pravila

   HP održava globalno primjenjiva pravila, standarde i postupke namijenjene zaštiti podataka tvrtke HP i klijenata. Pojedinosti sigurnosnih pravila tvrtke HP povjerljive su naravi radi zaštite integriteta podataka i sustava tvrtke HP. Međutim, u nastavku se navode sažeci naših osnovnih pravila.

2. Organizacija zaštite podataka

   Program zaštite podataka tvrtke HP osmišljen je za usmjeravanje i održavanje strategije i kontrole zaštite podataka u organizaciji. Ovaj sustav jamči usklađenost sigurnosnih pravila i kontrola tvrtke HP u cijeloj tvrtki, kao i poštivanje sigurnosnih zahtjeva svojih klijenata. Strukturiran u skladu sa sustavima kibernetičke sigurnosti koji su industrijski standard, zakonima i propisima, sustav se revidira svake godine kako bi se prilagodio razvoju prijetnji na razini tvrtke HP.

3. Upravljanje rizicima po kibernetičku sigurnost

   Program tvrtke HP za upravljanje rizicima po kibernetičku sigurnost osmišljen je tako da čuva povjerljivost, integritet i dostupnost svojih podataka. Program pruža dosljedan pristup identificiranju, procjeni, određivanju prioriteta, postupanju, otklanjanju, praćenju i izvješćivanju o rizicima po kibernetičku sigurnost. HP definira svoju sklonost rizicima kao prihvatljivu razinu izloženosti gubicima, a toleranciju na rizike kao stupanj odstupanja od te sklonosti. Rizici se procjenjuju uporabom definirane metodologije, što tvrtki HP omogućuje ublažavanje opasnosti po sigurnost podataka na prihvatljivu razinu. Ovaj program usklađen je s postupkom upravljanja rizicima poduzeća koji se primjenjuje u tvrtki HP.

Posljednje ažuriranje: Rujan 2024.

4. Zaštita ljudskih resursa

   Pravila tvrtke HP o zaštiti ljudskih resursa osiguravaju zaštitu podataka u cjelokupnoj karijeri zaposlenika uspostavom postupaka za pristup objektima, informacijskim sustavima i drugim resursima. To uključuje dobivanje pisanih potvrda putem ugovora o povjerljivosti i tajnosti, kao i provođenje postupaka provjere popratnih osobnih podataka. Svi kandidati za zapošljavanje u tvrtki HP moraju proći provjeru popratnih osobnih podataka u skladu s relevantnim zakonima, propisima i etikom.

5. Upravljanje resursima

   HP ima postupak za identifikaciju tehničkih informacijskih resursa, kategorizaciju ključnih resursa i održavanje dokumentiranih postupaka rukovanja za svaku vrstu klasifikacije podataka, uključujući one koji sadrže osobne podatke. Ti postupci obuhvaćaju pohranu, prijenos, komunikaciju, pristup, bilježenje, zadržavanje, uništavanje, odlaganje, upravljanje incidentima i izvješćivanje o kršenju pravila. Sigurnosna pravila i standardi tvrtke HP odnose se i na sigurno odlaganje medija.

6. Sigurnost podataka

   Program za zaštitu podataka tvrtke HP ocrtava sigurnosne prakse i tehničke kontrole koje se moraju primijeniti kako bi se zaštitila povjerljivost, autentičnost i integritet podataka. Pravni zahtjevi, vrijednost, značaj i osjetljivost na neovlašteno otkrivanje ili preinaku samo su neki od čimbenika koji određuju kako se podaci klasificiraju prema pravilima tvrtke HP o zaštiti sigurnosti podataka. Osim postupaka rukovanja podacima, u pravilima se navode šifriranje, brisanje, prikupljanje i obrada, zadržavanje, sigurnosno kopiranje i sprječavanje gubitka podataka.

7. Kontrola pristupa

   HP upotrebljava načelo najmanje povlastice za logičnu kontrolu pristupa, pružajući korisnički pristup putem jedinstvenih korisničkih ID-ova i lozinki. Pravilo za lozinke određuje složenost, snagu, valjanost i kontrole povijesti lozinki. Prava pristupa povremeno se preispituju i opozivaju nakon odlaska osoblja. Dogovoreni postupci za stvaranje i brisanje korisničkog računa provode se kako bi se odobrio i opozvao pristup korisničkim sustavima tijekom angažmana.

8. Šifriranje

   HP je definirao skup snažnih postupaka za šifriranje kako bi osigurao povjerljivost, integritet i dostupnost podatkovnih resursa. Odobreni protokoli zahtijevaju šifriranje za određene resurse, uključujući one koji sadrže osobne podatke. Naš program šifriranja uključuje uporabu matematičkih tehnika za osiguranje podataka i komunikacija, osiguravajući da samo ovlaštene strane mogu pristupiti podacima. Ključna komponenta programa za zaštitu podataka tvrtke HP jest zaštita podataka od neovlaštenog pristupa i izmjene.

9. Zaštita na radu i zaštita okoliša

   Objekti tvrtke HP osigurani su različitim fizičkim i elektroničkim kontrolama pristupa, uključujući zaštitare, elektronički nadzor pristupa i videonadzor (CCTV). Objekti su također opremljeni potrebnom infrastrukturnom podrškom, uključujući regulaciju temperature i pomoćna napajanja, s pomoću uređaja UPS i/ili dizel generatora za potporu ključnim uslugama. Svo osoblje tvrtke HP registrirano je i mora nositi odgovarajuće identifikacijske oznake.

10. Upravljanje operacijama

    HP je uspostavio minimalne zahtjeve za poboljšanje tehnološke infrastrukture, uključujući radne stanice, poslužitelje i mrežnu opremu. Ovi uređaji upotrebljavaju unaprijed poboljšane slike operacijskog sustava, a zahtjevi se razlikuju ovisno o operacijskom sustavu i implementiranim kontrolama. Dodatno, HP je postavio sustave za otkrivanje/sprječavanje neovlaštenog upada u mrežu (NIDS/NIPS) koji se nadziru i kojima se upravlja bez prekida (24/7).

11. Sigurnost komunikacija

    Sigurnost komunikacija jamči zaštitu podataka unutar korporacijskih mreža. To uključuje instalaciju i upravljanje mrežnim sigurnosnim komponentama (npr. vatrozid), odvajanje mreža, kao i filtriranje mreže i nadzor rukovanja e-poštom. Dodatno, uključuje nadzor i upravljanje komunikacijskim kanalima za otkrivanje i sprječavanje neovlaštenog pristupa ili kršenja pravila za zaštitu podataka.

12. Zaštita sustava

    Pravilima tvrtke HP propisuje se sigurna razvojna metodologija za sustave i softver tijekom njihova vijeka trajanja. Vijek trajanja razvoja softvera obuhvaća započinjanje, razvoj/nabavu, implementaciju, operacije i odlaganje. Sve komponente sustava ocjenjuju se u odnosu na njihov utjecaj na ukupnu sigurnost. HP je uspostavio kontrole za transakcije aplikacijskih usluga, uključujući provjeru vjerodajnica korisnika, digitalne potpise, šifriranje, sigurne komunikacijske protokole i pohranu pojedinosti o transakciji unutar odgovarajuće sigurnosne zone mreže. Obavljaju se i redovita interna skeniranja ranjivosti.

13. Treće strane i podizvođači

    HP ima postupke za odabir podizvođača koji ispunjavaju sveobuhvatne ugovorne sigurnosne zahtjeve. Za odgovarajuće dobavljače koji rukuju podacima tvrtke HP ili njezinih klijenata ili pristupaju mreži tvrtke HP, služba kibernetičke zaštite tvrtke HP provodi procjenu rizika kako bi se provjerio program zaštite podataka fizičkim, tehničkim i administrativnim zaštitnim mjerama. Ova je procjena obvezna kako bi dobavljač mogao pristupiti podacima tvrtke HP.

14. Upravljanje incidentima povezanim s povredama pravila o zaštiti podataka

    HP posjeduje sveobuhvatan postupak upravljanja kibernetičkim incidentima koji opisuje svrhu, opseg, uloge, odgovornosti, obvezu upravljanja, organizacijsku koordinaciju, postupke implementacije i provjeru usklađenosti. Ovaj se postupak pregledava i ažurira godišnje. Tim za odgovor na kibernetičke incidente, uključujući osoblje za kibernetičku sigurnost tvrtke HP obučeno za odgovor na incidente i upravljanje kriznim situacijama, provodi redovito preispitivanje simuliranih procesa i svih incidenata ili događaja.

15. Upravljanje kontinuiranim poslovanjem

    Globalni program kontinuiteta rada tvrtke HP osigurava potpuni kontinuitet kroz suradničke, standardizirane i dokumentirane postupke planiranja. Tvrtka povremeno ispituje svoje planove kontinuiranog poslovanja kako bi osigurala učinkovitost, testiranjem i ažuriranjem svih planova najmanje jednom godišnje. Osim toga, svo osoblje uključeno u plan kontinuiteta poslovanja prolazi odgovarajuću obuku.

16. Sukladnost

    Sukladnost oblikuje pristup tvrtke HP ispunjavanju zakonskih, ugovornih i internih očekivanja za učinkovit program za zaštitu podataka. Redoviti pregledi sustava za zaštitu podataka osiguravaju integraciju protokola u poslovanje svake poslovne grupe. U postupku pregleda također se ažuriraju dokumenti kako bi odražavali trenutačne zakonske obveze kako se zahtjevi razvijaju.

17. Industrija platnih kartica

    Okvir industrije platnih kartica (PCI) usmjerava pristup tvrtke HP postizanju usklađenosti sa standardom PCI, ocrtavajući poslovne odgovornosti i sigurnosne kontrole usklađene s PCI DSS-om. Instaliranjem i održavanjem kontrola za zaštitu mreže, poput vatrozida, HP osigurava ispunjavanje zahtjeva usklađenosti s PCI-jem.

18. Sigurnost proizvoda tvrtke HP

    Sigurnost proizvoda tvrtke HP obuhvaća bitne postupke za zaštitu proizvoda tvrtke HP, kao što je šifrirano potpisivanje, upravljanje sigurnosnim propustima proizvoda, izdavanje sigurnosnih biltena i prijavljivanje sigurnosnih problema u vezi s proizvodom. Te mjere osiguravaju da su proizvodi tvrtke HP sigurni i pouzdani korisnicima. Sigurnost proizvoda od najvećeg je značaja u tvrtki HP jer pomaže da se održi povjerenje klijenata i štiti od potencijalnih prijetnji.

19. Sigurnost usluga tvrtke HP

    Sigurnost usluga tvrtke HP obuhvaća bitne postupke za zaštitu usluga koje se pružaju klijentima tvrtke HP. Ova se pravila odnose na različita područja sigurnosti usluga, uključujući okruženja hostirana na infrastrukturi tvrtke HP, hostirana od strane trećih strana, od strane partnera i od strane klijenata. Te mjere osiguravaju da usluge tvrtke HP ostanu sigurne i pouzdane korisnicima. Implementacijom snažne sigurnosne prakse, HP osigurava zaštitu i integritet svojih proizvoda i usluga, omogućujući sigurno i pouzdano okruženje svim korisnicima.