REZIME BEZBEDNOSNIH MERA KOMPANIJE HP

Da bi zaštitila podatke klijenata, kompanija HP se pridržava opsežnog skupa kontrola bezbednosti informacija, uključujući smernice, prakse, procedure i organizacione strukture, kako bi zaštitila poverljivost, integritet i dostupnost informacija koje pripadaju njoj i njenim klijentima (uključujući lične podatke kako je definisano u Dodatku o obradi podataka klijenata kompanije HP). U nastavku je naveden pregled tehničkih/organizacionih bezbednosnih mera koje se primenjuju na nivou kompanije HP.

1. Bezbednosne smernice

   HP održava globalno primenljive smernice, standarde i procedure za zaštitu podataka kompanije HP i njenih klijenata. Detalji bezbednosnih smernica kompanije HP su poverljivi radi zaštite integriteta njenih sistema i podataka. Međutim, rezimei naših ključnih smernica su navedeni u nastavku.

2. Uspostavljanje bezbednosti informacija

   Svrha programa bezbednosti informacija kompanije HP je vođenje i održavanje strategije i kontrola bezbednosti informacija organizacije. Ovaj sistem osigurava usaglašenost celog preduzeća sa bezbednosnim smernicama i kontrolama kompanije HP, kao i poštovanje bezbednosnih zahteva njenih klijenata. Ovaj radni okvir, strukturiran u skladu sa industrijski standardnim okvirima za kibernetičku bezbednost, zakonima i propisima, pregleda se svake godine kako bi se prilagodio novonastalim pretnjama po kompaniju HP.

3. Upravljanje rizicima po kibernetičku bezbednost

   Svrha programa za upravljanje rizicima po kibernetičku bezbednost kompanije HP je očuvanje poverljivosti, integriteta i dostupnosti njenih informacionih resursa. Program pruža dosledan pristup identifikovanju, proceni, određivanju prioriteta, otklanjanju, praćenju i prijavljivanju rizika po kibernetičku bezbednost, kao i rukovanju njima. HP definiše svoj apetit za rizik kao prihvatljiv nivo izloženosti gubicima i tolerancije rizika kao stepen odstupanja od ovog apetita. Rizici se procenjuju pomoću definisane metodologije, što kompaniji HP omogućava da svede rizike po bezbednost informacija na prihvatljiv nivo. Ovaj program je usklađen sa procesom kompanije HP za upravljanje rizicima preduzeća.

4. Bezbednost ljudskih resursa

   Smernice za bezbednost ljudskih resursa kompanije HP obezbeđuju bezbednost informacija tokom čitavog radnog ciklusa zaposlenih uspostavljanjem procesa za pristup objektima, informacionim sistemima i drugim resursima. To uključuje pribavljanje pismenih potvrda putem ugovora o poverljivosti i neotkrivanju podataka, kao i sprovođenje procedura provere kvalifikacija. Obavezna je provera kvalifikacija svih kandidata za zaposlenje u kompaniji HP u skladu sa relevantnim zakonima, propisima i etikom.

5. Upravljanje resursima

   HP ima proces za identifikaciju resursa u vidu tehničkih informacija, kategorizaciju ključnih resursa i održavanje dokumentovanih procedura rukovanja za svaki tip klasifikacije informacija, uključujući one sa ličnim podacima. Te procedure pokrivaju skladištenje, prenos, komunikaciju, pristup, evidentiranje, zadržavanje, uništavanje, odlaganje, upravljanje incidentima i obaveštenje o prekršajima. Bezbednosne smernice i standardi kompanije HP nalažu i bezbedno odlaganje medija.

6. Bezbednost podataka

   Program za bezbednost podataka kompanije HP opisuje bezbednosne prakse i tehničke kontrole koje se moraju primenjivati u cilju zaštite poverljivosti, verodostojnosti i integriteta podataka. Zakonske obaveze, vrednost, značaj i osetljivost na neovlašćeno otkrivanje ili izmene su neki od faktora koji određuju način klasifikovanja informacija prema smernicama za bezbednost podataka kompanije HP. Pored procedura za rukovanje podacima, ove smernice regulišu šifrovanje podataka, brisanje, prikupljanje i obradu, zadržavanje, pravljenje rezervnih kopija i sprečavanje gubitka podataka.

7. Kontrola pristupa

   HP primenjuje princip najmanje privilegije za logičku kontrolu pristupa, pružajući pristup korisnicima preko jedinstvenih korisničkih ID-ova i lozinki. Smernice za lozinke definišu kontrole složenosti, jačine, valjanosti i istorije lozinki. Prava pristupa se povremeno revidiraju i ukidaju po odlasku osoblja. Dogovorene procedure za kreiranje i brisanje korisničkih naloga se primenjuju za odobravanje i opozivanje pristupa klijentskim sistemima tokom rada.

8. Kriptografija

   Kompanija HP je definisala skup opsežnih procesa za kriptografiju kako bi osigurala poverljivost, integritet i dostupnost informacionih resursa. Odobreni protokoli zahtevaju šifrovanje za određene resurse, uključujući one sa ličnim podacima. Naš kriptografski program uključuje upotrebu matematičkih tehnika za zaštitu informacija i komunikacija, čime se osigurava da samo ovlašćene strane imaju pristup podacima. Ključna komponenta programa bezbednosti informacija kompanije HP je zaštita podataka od neovlašćenog pristupa i izmena.

9. Fizička i ekološka bezbednost

   Objekti kompanije HP su zaštićeni putem različitih fizičkih i elektronskih kontrola pristupa, uključujući radnike obezbeđenja, elektronsku kontrolu pristupa i zatvoren sistem za prenos signala (closed-circuit television – CCTV). Objekti imaju i neophodnu infrastrukturnu podršku, uključujući kontrolu temperature i rezervne opcije napajanja, u vidu neprekidnog napajanja (UPS) i/ili dizel generatora za podršku ključnim uslugama. Svo osoblje kompanije HP je registrovano i mora da nosi odgovarajuće identifikacione oznake.

10. Upravljanje operacijama

    Kompanija HP je uspostavila minimalne bezbednosne zahteve za tehnološku infrastrukturu, uključujući radne stanice, servere i mrežnu opremu. Ti uređaji koriste unapred zaštićene slike operativnog sistema, sa zahtevima koji se razlikuju u zavisnosti od operativnog sistema i primenjenih kontrola. Osim toga, kompanija HP primenjuje sisteme za otkrivanje/sprečavanje neovlašćenog pristupa mreži (NIDS/NIPS) koji se non-stop nadgledaju i kontrolišu.

11. Bezbednost komunikacija

    Bezbednost komunikacija pruža zaštitu informacija unutar korporativnih mreža. To uključuje instalaciju komponenti mrežne bezbednosti (npr. zaštitni zidovi) i upravljanje njima, podelu mreža, kao i veb filtriranje i kontrole rukovanja e-poštom. Obuhvata i praćenje i kontrolu kanala komunikacije radi otkrivanja i sprečavanja neovlašćenog pristupa ili povreda bezbednosti podataka.

12. Bezbednost sistema

    Smernice kompanije HP nalažu bezbednu metodologiju razvoja sistema i softvera tokom njihovog životnog ciklusa. Životni ciklus razvoja softvera obuhvata pokretanje, razvoj/pribavljanje, primenu, operacije i odlaganje. Procenjuje se uticaj svih komponenti sistema na sveopštu bezbednost. Kompanija HP je uspostavila kontrole za uslužne transakcije preko aplikacija, uključujući proveru valjanosti akreditiva korisnika, digitalne potpise, šifrovanje, bezbedne komunikacione protokole i čuvanje detalja transakcija u odgovarajućoj zoni bezbednosti mreže. Sprovode se i redovna interna skeniranja ranjivosti.

13. Treće strane i podizvođači

    Kompanija HP ima procese za izbor podizvođača koji ispunjavaju sveobuhvatne ugovorne bezbednosne zahteve. Za odgovarajuće dobavljače koji rukuju podacima kompanije HP ili njenih klijenata ili pristupaju HP mreži, odeljenje kompanije HP za kibernetičku bezbednost sprovodi procenu rizika u cilju provere programa bezbednosti informacija sa fizičkim, tehničkim i administrativnim merama zaštite. Ta procena mora da se izvede da bi dobavljač mogao da pristupi informacijama kompanije HP.

14. Upravljanje incidentima u oblasti bezbednosti informacija

    Kompanija HP ima sveobuhvatan proces upravljanja incidentima u oblasti kibernetičke bezbednosti koji reguliše svrhu, obim, uloge, odgovornosti, učešće rukovodstva, organizacionu koordinaciju, procedure primene i proveru usaglašenosti. Ovaj proces se svake godine pregleda i ažurira. Tim zadužen za incidente u oblasti kibernetičke bezbednosti, uključujući osoblje kompanije HP za kibernetičku bezbednost obučeno za reagovanje na incidente i upravljanje kriznim situacijama, sprovodi redovne kontrolne provere procesa i svih incidenata ili događaja.

15. Upravljanje kontinuitetom poslovanja

    Globalni program kontinuiteta operacija kompanije HP pruža sveobuhvatni kontinuitet kroz kolaborativne, standardizovane i dokumentovane procese planiranja. Kompanija povremeno sprovodi planove za kontinuitet poslovanja kako bi osigurala efikasnost, testiranje i ažuriranje svih planova najmanje jednom godišnje. Osim toga, celokupno osoblje uključeno u plan kontinuiteta poslovanja prolazi kroz odgovarajuću obuku.

16. Usaglašenost

    Usaglašenost oblikuje pristup kompanije HP ispunjavanju zakonskih, ugovornih i internih očekivanja za efikasan program bezbednosti informacija. Redovnim pregledima bezbednosti informacija osigurava se integrisanost protokola u operacije svake poslovne grupe. Procesom pregleda se osigurava i da su dokumenti uvek ažurni kako bi odražavali aktuelne zakonske obaveze paralelno sa razvojem zahteva.

17. Industrija platnih kartica

    Radni okvir industrije platnih kartica (PCI) usmerava pristup kompanije HP postizanju usaglašenosti sa PCI zahtevima, pri čemu reguliše poslovne odgovornosti i bezbednosne kontrole usklađene sa bezbednosnim standardom za podatke sa platnih kartica (PCI DSS). Instaliranjem i održavanjem kontrola za mrežnu bezbednost, kao što su zaštitni zidovi, HP osigurava da ispunjava zahteve usaglašenosti sa PCI zahtevima.

18. Bezbednost proizvoda kompanije HP

    Bezbednost proizvoda kompanije HP obuhvata osnovne prakse za zaštitu HP proizvoda, kao što su potpisivanje kodom, upravljanje bezbednosnim ranjivostima proizvoda, izdavanje bezbednosnih biltena i prijavljivanje bezbednosnih problema sa proizvodom. Zahvaljujući tim merama HP proizvodi su bezbedni i pouzdani za korisnike. Bezbednost proizvoda je od suštinskog značaja za kompaniju HP jer doprinosi očuvanju poverenja klijenata i štiti od potencijalnih pretnji.

19. Bezbednost usluga kompanije HP

    Bezbednost usluga kompanije HP obuhvata osnovne prakse za zaštitu usluga koje se pružaju njenim klijentima. Te smernice se odnose na različite oblasti bezbednosti usluga, uključujući okruženja koja hostuje HP infrastruktura, okruženja koja hostuju treće strane, okruženja koja hostuju partneri i okruženja koja hostuju klijenti. Zahvaljujući tim merama HP usluge su bezbedne i pouzdane za korisnike. Primenom opsežnih bezbednosnih praksi, HP osigurava bezbednost i integritet svojih proizvoda i usluga, pružajući bezbedno i pouzdano okruženje za sve korisnike.

Poslednji put ažurirano: Septembar 2024.