HP SAUGOS PRIEMONIŲ SUVESTINĖ

Siekdama apsaugoti klientų duomenis, HP laikosi patikimų informacijos saugumo kontrolės priemonių, įskaitant politiką, praktiką, procedūras ir organizacines struktūras, kad apsaugotų savo ir klientų informacijos (įskaitant asmeninius duomenis, kaip apibrėžta HP klientų ir duomenų tvarkymo dokumento papildymuose) konfidencialumą, vientisumą ir prieinamumą. Toliau pateikiama HP techninių / organizacinių saugumo priemonių visoje bendrovėje apžvalga.

1. Saugumo politika

   HP vykdo pasauliniu mastu taikomą politiką, standartus ir procedūras, skirtas HP ir klientų duomenims apsaugoti. Siekiant apsaugoti HP duomenų ir sistemų vientisumą, išsamesnės HP saugumo politikos nuostatos yra konfidencialios. Tačiau toliau pateikiamos pagrindinių mūsų politikos nuostatų santraukos.

2. Organizacijos informacijos saugumas

   HP informacijos saugumo programa skirta valdyti ir palaikyti organizacijos informacijos saugumo strategiją ir kontrolės priemones. Ši sistema užtikrina, kad visoje bendrovėje būtų laikomasi HP saugumo politikos ir kontrolės priemonių, taip pat jos klientų saugumo reikalavimų. Sistemos struktūra suderinta su pramonėje taikomomis kibernetinio saugumo sistemomis, įstatymais ir reglamentais, ji kasmet peržiūrima, kad būtų pritaikyta prie besikeičiančios HP grėsmių aplinkos.

3. Kibernetinio saugumo rizikos valdymas

   HP kibernetinio saugumo rizikos valdymo programa skirta informacijos išteklių konfidencialumui, vientisumui ir prieinamumui išsaugoti. Programoje numatytas nuoseklus požiūris į kibernetinio saugumo rizikos nustatymą, vertinimą, prioritetų nustatymą, apdorojimą, šalinimą, stebėjimą ir ataskaitų teikimą. HP savo priimtiną riziką apibrėžia kaip priimtiną rizikos lygį, o rizikos toleranciją - kaip nukrypimo nuo šio lygio laipsnį. Rizika vertinama pagal nustatytą metodiką, todėl HP gali sumažinti informacijos saugumo riziką iki priimtino lygio. Ši programa suderinta su HP įmonės rizikos valdymo procesu.

4. Žmogiškųjų išteklių sauga

   HP Žmogiškųjų išteklių saugumo politika užtikrina informacijos saugumą per visą darbuotojo veiklos ciklą, nustatydama prieigos prie patalpų, informacinių sistemų ir kitų išteklių procesus. Tai apima raštiškų patvirtinimų gavimą sudarant konfidencialumo ir informacijos neatskleidimo susitarimus, taip pat atliekant biografijos faktų tikrinimo procedūras. Visi kandidatai, norintys įsidarbinti HP, privalo atlikti biografijos faktų patikrinimą pagal atitinkamus įstatymus, taisykles ir etikos normas.

5. Išteklių valdymas

   HP yra įdiegusi techninių informacinių išteklių nustatymo, svarbiausių išteklių skirstymo į kategorijas ir dokumentais pagrįstų kiekvieno informacijos klasifikavimo tipo, įskaitant tuos, kuriuose yra asmens duomenų, tvarkymo procedūrų tvarką. Šios procedūros apima saugojimą, perdavimą, ryšį, prieigą, registravimą, saugojimą, naikinimą, šalinimą, incidentų valdymą ir pranešimą apie pažeidimą. HP saugumo politika ir standartai taip pat įpareigoja saugiai šalinti laikmenas.

6. Duomenų saugumas

   HP Duomenų saugumo programoje aprašoma saugumo praktika ir techninės kontrolės priemonės, kurios turi būti įdiegtos siekiant apsaugoti duomenų konfidencialumą, autentiškumą ir vientisumą. Teisiniai reikalavimai, vertė, svarbumas ir įautrumas neteisėtam atskleidimui ar modifikavimui - tai tik keli veiksniai, lemiantys, kaip informacija klasifikuojama pagal HP duomenų saugumo politiką. Politikoje aprašomos ne tik duomenų tvarkymo procedūros, bet ir duomenų šifravimas, ištrynimas, rinkimas ir tvarkymas, saugojimas, atsarginių kopijų darymas ir duomenų praradimo prevencija.

7. Prieigos valdymas

   Loginės prieigos valdymui HP taiko mažiausių teisių principą, suteikdama naudotojui prieigą per unikalius naudotojo ID ir slaptažodžius. Slaptažodžių politikoje apibrėžiamos sudėtingumo, stiprumo, galiojimo ir slaptažodžių istorijos kontrolės priemonės. Prieigos teisės periodiškai peržiūrimos ir panaikinamos personalui išvykus. Siekiant suteikti ir atšaukti prieigą prie kliento sistemų atliekant užduotis, įdiegtos suderintos naudotojo paskyrų kūrimo ir panaikinimo procedūros.

8. Kriptografija

   HP nustatė patikimų kriptografijos procesų rinkinį, kad užtikrintų informacijos išteklių konfidencialumą, vientisumą ir prieinamumą. Patvirtintuose protokoluose reikalaujama šifruoti tam tikrus išteklius, įskaitant tuos, kuriuose yra asmens duomenų. Mūsų Kriptografijos programa apima matematinių metodų naudojimą informacijai ir ryšiams apsaugoti, užtikrinant, kad duomenis galėtų pasiekti tik įgaliotos šalys. Svarbiausias HP informacijos saugumo programos komponentas yra duomenų apsauga nuo neteisėtos prieigos ir klastojimo.

9. Fizinis ir aplinkos saugumas

   HP įrenginiai yra apsaugoti naudojant įvairias fizines ir elektronines prieigos kontrolės priemones, įskaitant apsaugos darbuotojus, elektroninę prieigos kontrolę ir vaizdo stebėjimo kameras (CCTV). Patalpose taip pat įrengta būtina infrastruktūra, įskaitant temperatūros kontrolę ir atsarginį maitinimą, naudojant UPS / dyzelinius generatorius svarbiausioms funkcijoms palaikyti. Visi HP darbuotojai yra užregistruoti ir privalo turėti atitinkamus identifikavimo ženklelius.

10. Operacijų valdymas

    HP nustatė minimalius technologijų infrastruktūros, įskaitant darbo stotis, serverius ir tinklo įrangą, apsaugos reikalavimus. Šiuose įrenginiuose naudojami iš anksto paruošti operacinės sistemos atvaizdai, kurių reikalavimai skiriasi priklausomai nuo operacinės sistemos ir įdiegtų valdiklių. Be to, HP įdiegė įsilaužimų į tinklą aptikimo ir prevencijos sistemas (NIDS/NIPS), kurios stebimos ir valdomos 24 valandas per parą, 7 dienas per savaitę.

11. Ryšių saugumas

    Ryšių saugumas užtikrina informacijos apsaugą įmonės tinkluose. Tai apima tinklo saugumo komponentų (pvz., ugniasienių) diegimą ir valdymą, tinklų atskyrimą, taip pat žiniatinklio filtravimo ir el. pašto tvarkymo kontrolę. Be to, ji apima ryšių kanalų stebėseną ir valdymą, kad būtų galima nustatyti neteisėtą prieigą ar duomenų saugos pažeidimus ir užkirsti jiems kelią.

12. Sistemų saugumas

    HP politika įpareigoja taikyti saugią sistemų ir programinės įrangos kūrimo metodiką per visą jų gyvavimo ciklą. Programinės įrangos kūrimo gyvavimo ciklas apima inicijavimą, kūrimą / įsigijimą, įgyvendinimą, eksploatavimą ir šalinimą. Įvertinamas visų sistemos komponentų poveikis bendram saugumui. HP nustatė taikomųjų programų paslaugų sandorių kontrolės priemones, įskaitant naudotojo įgaliojimų patvirtinimą, skaitmeninius parašus, šifravimą, saugius ryšio protokolus ir sandorio duomenų saugojimą atitinkamoje tinklo saugumo zonoje. Taip pat reguliariai atliekami vidaus pažeidžiamumo patikrinimai.

13. Trečiosios šalys ir subrangovai

    HP taiko procesus, skirtus atrinkti subrangovus, kurie atitinka išsamius sutartinius saugumo reikalavimus. HP Kibernetinis saugumas atlieka atitinkamų tiekėjų, tvarkančių HP ar klientų duomenis arba turinčių prieigą prie HP tinklo, rizikos vertinimą, kad patikrintų informacijos saugumo programą naudojant fizines, technines ir administracines apsaugos priemones. Šis vertinimas atliekamas prieš tiekėjui suteikiant prieigą prie HP informacijos.

14. Informacijos saugumo incidentų valdymas

    HP turi išsamų kibernetinių incidentų valdymo procesą, kuriame nurodytas tikslas, taikymo sritis, vaidmenys, atsakomybė, vadovybės įsipareigojimas, organizacinis koordinavimas, įgyvendinimo procedūros ir atitikties tikrinimas. Šis procesas kasmet peržiūrimas ir atnaujinamas. Reagavimo į kibernetinius incidentus grupė, į kurią įeina HP kibernetinio saugumo darbuotojai, apmokyti reaguoti į incidentus ir valdyti krizes, reguliariai kartu atlieka proceso ir visų incidentų ar įvykių apžvalgas.

15. Veiklos tęstinumo valdymas

    Visuotinė HP veiklos tęstinumo programa užtikrina veiklos tęstinumą bendradarbiaujant, taikant standartizuotus ir dokumentais pagrįstus planavimo procesus. Bendrovė periodiškai tikrina savo veiklos tęstinumo planus, kad užtikrintų jų veiksmingumą, bent kartą per metus testuodama ir atnaujindama visus planus. Be to, visiems su veiklos tęstinumo planu susijusiems darbuotojams suteikiami atitinkami mokymai.

16. Atitiktis

    Atitiktis formuoja HP požiūrį į teisinių, sutartinių ir vidinių lūkesčių, susijusių su veiksminga informacijos saugumo programa, tenkinimą. Reguliari informacijos saugumo peržiūra užtikrina, kad protokolai būtų integruoti į kiekvienos įmonės grupės veiklą. Atliekant peržiūrą dokumentai taip pat atnaujinami, kad atspindėtų dabartinius teisinius įsipareigojimus, nes reikalavimai keičiasi.

17. Mokėjimo kortelių pramonė

    Mokėjimo kortelių pramonės (PCI) sistema grindžiamas HP požiūris į PCI atitikties užtikrinimą, nurodant verslo atsakomybę ir saugumo kontrolės priemones, suderintas su PCI DSS. Diegdama ir prižiūrėdama tinklo saugumo kontrolės priemones, pvz., ugniasienes, HP užtikrina, kad ji atitinka PCI atitikties reikalavimus.

18. HP produktų saugumas

    „HP“ produktų saugumas apima esmines HP produktų saugumo užtikrinimo praktikas, tokias kaip kodo pasirašymas, produktų saugumo pažeidžiamumo valdymas, saugumo biuletenių leidyba ir pranešimai apie produktų saugumo problemas. Šios priemonės užtikrina, kad HP produktai išliktų saugūs ir patikimi naudotojams. HP itin svarbus gaminių saugumas, nes jis padeda išlaikyti klientų pasitikėjimą ir apsaugo nuo galimų grėsmių.

19. HP Paslaugų saugumas

    HP Paslaugų saugumas apima esminius HP klientams teikiamų paslaugų saugumo užtikrinimo būdus. Šioje politikoje aptariamos įvairios paslaugų saugumo sritys, įskaitant HP infrastruktūros prieglobą, trečiosios šalies prieglobą, partnerių prieglobą ir kliento prieglobą. Šiomis priemonėmis užtikrinama, kad HP paslaugos naudotojams išliktų saugios ir patikimos. Įgyvendindama patikimą saugumo praktiką, HP užtikrina savo produktų ir paslaugų saugumą bei integralumą, taip kurdama saugią ir patikimą aplinką visiems naudotojams.

Paskutinį kartą atnaujinta: 2024 m. rugsėjo mėn.