HP DROŠĪBAS PASĀKUMU KOPSAVILKUMS

Lai aizsargātu Klienta datus, HP ievēro stingru informācijas drošības kontroles sistēmu, kas ietver politiku, praksi, procedūras un organizācijas struktūras, lai aizsargātu savas un klienta informācijas konfidencialitāti, integritāti un pieejamību (tostarp Personas datus, kas noteikti HP Klientu un datu apstrādes papildprogrammā). Tālāk ir sniegts pārskats par HP tehniskajiem/organizācijas drošības pasākumiem visā uzņēmumā.

1. Drošības politika

   HP uztur vispārēji piemērojamas politikas, standartus un procedūras, kas paredzētas HP un Klientu datu aizsardzībai. HP drošības politiku detalizācijas pakāpe ir konfidenciāla, lai aizsargātu HP datu un sistēmu integritāti. Tomēr mūsu galveno politiku kopsavilkumi ir iekļauti tālāk.

2. Informācijas drošības organizēšana

   HP informācijas drošības programma ir izveidota, lai vadītu un uzturētu organizācijas informācijas drošības stratēģiju un vadības ierīces. Šī sistēma nodrošina uzņēmuma atbilstību HP drošības politikām un kontrolēm, kā arī to, ka tiek ievērotas klientu drošības prasības. Sistēma tiek pārskatīta katru gadu, lai pielāgotos HP pieaugušo draudu ainavai, kas ir saderīga ar nozares standarta kiberdrošības sistēmu, normatīviem un noteikumiem.

3. Kiberdrošības risku pārvaldība

   HP kiberdrošības risku pārvaldības programma ir izstrādāta, lai saglabātu informācijas līdzekļu konfidencialitāti, integritāti un pieejamību. Šī programma nodrošina konsekventu pieeju kiberdrošības risku identificēšanai, novērtēšanai, prioritāšu noteikšanai, ārstēšanai, labošanai, izsekošanai un informēšanai par tiem. HP nosaka savu Risku apetīti kā pieņemamu zaudējumu risku un Risku pielaides līmeni kā šīs apetītes variācijas pakāpi. Riskus novērtē, izmantojot noteiktu metodiku, kas ļauj HP atklāt drošības riskus, kas saistīti ar informācijas drošību līdz pieņemamam līmenim. Šī programma ir saderīga ar HP uzņēmumu risku pārvaldības procesu.

4. HR drošība

   HP cilvēku resursu drošības politika garantē informācijas drošību visā darbinieku dzīves cikla laikā, izveidojot procesus, kā piekļūt iekārtām, informācijas sistēmām un citiem pamatlīdzekļiem. Tas ietver rakstiskas garantijas, izmantojot konfidencialitātes un neizpaušanas līgumus, kā arī veicot pamata skrīninga procedūras. Visiem kandidātiem, kuri tiks nodarbināti uzņēmumā HP, jāveic pamata pārbaude saskaņā ar attiecīgajiem tiesību aktiem, noteikumiem un ētikas standartiem.

5. Līdzekļu pārvaldība

   HP identificē tehniskās informācijas līdzekļus, nosaka kritiskus līdzekļus un uztur dokumentētas apstrādes procedūras katram informācijas klasifikācijas veidam, ieskaitot tās, kas satur Personas datus. Šīs procedūras attiecas uz glabāšanu, pārsūtīšanu, saziņu, piekļuvi, reģistrāciju, uzglabāšanu, iznīcināšanu, atbrīvošanos, incidentu pārvaldību un paziņojumu par pārkāpumiem. HP drošības politikas un standarti arī nosaka, kā drošā veidā atbrīvoties no materiāliem.

6. Datu drošība

   HP Datu drošības programmā ir ieskicēta drošības prakse un tehniskie kontroles pasākumi, kas jāīsteno, lai aizsargātu datu konfidencialitāti, autentiskumu un integritāti. Juridiskās prasības, vērtība, kritiskums un jutība pret nesankcionētu atklāšanu vai modificēšanu ir daži no faktoriem, kas nosaka, kā informācija tiek klasificēta saskaņā ar HP Datu drošības politiku. Papildus datu apstrādes procedūrām politikas iezīmē datu šifrēšanu, dzēšanu, apkopošanu un apstrādi, saglabāšanu, dublēšanu un datu zudumu novēršanu.

7. Piekļuves kontrole

   Loģiskās piekļuves kontrolei HP izmanto vismaz privilēģiju principu, kas nodrošina lietotāja piekļuvi, izmantojot unikālus lietotāja ID un paroles. Paroļu politika nosaka sarežģītību, stiprumu, derīgumu un paroļu vēstures kontroles pasākumus. Piekļuves tiesības tiek periodiski pārskatītas un atsauktas pēc darbinieku darba attiecību pārtraukšanas ar uzņēmumu. Tiek īstenotas saskaņotās lietotāja konta izveides un dzēšanas procedūras, lai piešķirtu un atsauktu piekļuvi klienta sistēmām darba laikā.

8. Kriptogrāfija

   HP ir definējis stingrus kriptogrāfijas procesus, lai nodrošinātu informācijas līdzekļu konfidencialitāti, integritāti un pieejamību. Apstiprinātiem protokoliem nepieciešama šifrēšana noteiktiem līdzekļiem, ieskaitot tos, kas satur personas datus. Mūsu kriptogrāfijas programma ietver matemātisko paņēmienu izmantošanu, lai nodrošinātu informācijas un sakaru drošību, nodrošinot, ka datiem var piekļūt tikai pilnvarotas personas. HP informācijas drošības programmas kritiskais komponents aizsargā datus no nesankcionētas piekļuves un viltojumiem.

9. Fiziskā un vides drošība

   HP iekārtas tiek aizsargātas, izmantojot dažādus fiziskas un elektroniskas piekļuves kontroles pasākumus, tostarp drošības sargus, elektroniskas piekļuves kontroles pasākumu un kabeļtelevīziju (CCTV). Iekārtas ir aprīkotas arī ar nepieciešamo infrastruktūras atbalstu, ieskaitot temperatūras kontroli un rezerves elektropadevi, UPS un/vai dīzeļģeneratorus, lai atbalstītu kritiskus pakalpojumus. Visi HP darbinieki ir reģistrēti, un viņiem ir jānēsā līdzi atbilstošas identifikācijas kartītes.

10. Darbību pārvaldība

    HP ir noteicis minimālās nostiprināšanas prasības tehnoloģiju infrastruktūrai, ieskaitot darbstacijas, serverus un tīkla aprīkojumu. Šīs ierīces izmanto iepriekš nostiprinātas operētājsistēmas attēlus, kuru prasības atšķiras atkarībā no operētājsistēmas un ieviestajiem kontroles pasākumiem. Turklāt HP ir izvietojis tīkla ielaušanās konstatēšanas/novēršanas sistēmas (NIDS/NIPS), kuras pārrauga un pārvalda 24/7.

11. Sakaru drošība

    Sakaru drošība nodrošina informācijas aizsardzību korporatīvajā tīklos. Tas ietver tīkla drošības komponentu (piemēram, ugunsmūru) instalēšanu un pārvaldību, tīklu segregāciju, kā arī tīmekļa filtrēšanas un e-pasta apstrādes kontroles pasākumus. Turklāt tā ietver sakaru kanālu pārraudzību un pārvaldību, lai konstatētu un novērstu nesankcionētu piekļuvi vai datu aizsardzības pārkāpumiem.

12. Sistēmu drošība

    HP politika nosaka drošu sistēmu un programmatūras izstrādes metodoloģiju visā to dzīves cikla laikā. Programmatūras attīstības dzīves cikls ietver uzsākšanu, izstrādi/iegādi, ieviešanu, darbību un atbrīvošanos. Tiek izvērtēta visu sistēmas komponentu ietekme uz vispārējo drošību. HP ir izveidojis vadības iestatījumus lietojumprogrammas pakalpojumu darbībām, tostarp lietotāja akreditācijas datu validēšanai, digitālajiem parakstiem, šifrēšanai, drošiem sakaru protokoliem un darbību detaļu saglabāšanai atbilstošajā tīkla drošības zonā. Tiek veikti arī parastās iekšējās neaizsargātības skenēšanas darbi.

13. Trešās puses un apakšuzņēmēji

    HP ir ieviesis procesus, kā izvēlēties apakšuzņēmējus, kuri ievēro visaptverošas līgumā noteiktās drošības prasības. Attiecībā uz spēkā esošajiem piegādātājiem, kas apstrādā HP vai klienta datus vai piekļūst HP tīklam, HP kiberdrošība veic riska novērtējumu, lai pārbaudītu informācijas drošības programmu ar fiziskiem, tehniskiem un administratīviem aizsardzības pasākumiem. Šis novērtējums ir nepieciešams, lai piegādātājs varētu piekļūt HP informācijai.

14. Informācijas drošības incidentu pārvaldība

    HP ir visaptverošs kiberincidentu pārvaldības process, kurā izklāstīts tā mērķis, piemērošanas joma, lomas, pienākumi, vadības apņemšanās, organizācijas koordinācija, īstenošanas procedūras un atbilstības pārbaude. Šo procesu pārskata un atjaunina katru gadu. Kiberincidentu reaģēšanas grupa, tostarp HP kiberdrošības personāls, kas ir apmācīts ar incidentu reaģēšanu un krīzes pārvaldību, regulāri pārskata procesu un visus incidentus vai notikumus.

15. Uzņēmējdarbības nepārtrauktības pārvaldība

    HP globālā darbību nepārtrauktības programma nodrošina nepārtrauktību no gala līdz galam, izmantojot sadarbības, standartizētus un dokumentējamus plānošanas procesus. Uzņēmums periodiski izmanto savas uzņēmējdarbības turpināšanas plānus, lai nodrošinātu efektivitāti, pārbaudes un atjauninātu visus plānus vismaz reizi gadā. Turklāt visi darbinieki, kas ir saistīti ar uzņēmējdarbības turpināšanas plānu, saņem atbilstošu apmācību.

16. Atbilstība

    Atbilstības nosaka HP pieeju, lai nodrošinātu atbilstību juridiskajām, līgumsaistībām un iekšējām gaidām par efektīvu informācijas drošības programmu. Regulāras informācijas drošības pārbaudes nodrošina, ka protokoli ir integrēti katras biznesa grupas darbībā. Pārskatīšanas procesā tiek arī atjaunināti dokumenti, lai atspoguļotu pašreizējos juridiskos pienākumus, jo prasības pieaug.

17. Maksājumu karšu nozare

    Maksājumu karšu nozares (PCI) sistēma nosaka HP pieeju, lai panāktu PCI atbilstības ievērošanu, kurā noteikti uzņēmējdarbības pienākumi un drošības kontrole, kas salāgota ar PCI DSS. Instalējot un uzturot tīkla drošību, piemēram, ugunsmūrus, HP nodrošina tā atbilstību PCI saderības prasībām.

18. HP produktu drošība

    HP produktu drošība ietver pamatpraksi HP produktu drošībai, piemēram, kodu parakstīšanu, produktu drošības neaizsargātības pārvaldību, drošības biļetenu izdošanu un iekārtas drošības problēmu uzrādīšanu. Šie pasākumi nodrošina, ka HP produkti ir droši un uzticami lietotājiem. Produktu drošība ir īpaši svarīga uzņēmumam HP, jo tā palīdz uzturēt klientu uzticēšanos un aizsargā pret iespējamiem draudiem.

19. HP pakalpojumu drošība

    HP pakalpojumu drošība ietver pamatpraksi, lai nodrošinātu HP klientiem sniegtos pakalpojumus. Šī politika attiecas uz dažādām pakalpojumu drošības jomām, tostarp uzņēmumā HP infrastruktūru, trešo pušu viesotajām, partneru viesotajām un klientu mitinātajām vidēm. Šie pasākumi nodrošina, ka HP pakalpojumi ir droši un uzticami lietotājiem. Īstenojot robustu drošības praksi, HP garantē savu produktu un pakalpojumu drošību un integritāti, veicinot drošu un uzticamu vidi visiem lietotājiem.