SAMMENFATNING AF HP'S SIKKERHEDSFORANSTALTNINGER

HP respekterer et robust sæt informationssikkerhedskontroller, herunder politikker, praksis, procedurer og organisatoriske strukturer for at sikre fortroligheden, integriteten og tilgængeligheden af sine egne og sine kunders oplysninger (herunder personlige data som defineret i HP's Addenda vedrørende kunde- og databehandling), for at beskytte kundedata. Følgende indeholder en oversigt over HP's tekniske/organisatoriske sikkerhedsforanstaltninger i hele virksomheden.

1. Sikkerhedspolitik

   HP vedligeholder globalt gældende politikker, standarder og procedurer, som er beregnet til at beskytte HP- og kundedata. Detaljerne i HP's sikkerhedspolitikker er fortrolige for at beskytte integriteten af HP's data og systemer. Resuméer af vores vigtigste politikker er dog indeholdt nedenfor.

2. Informationssikkerhedsorganisation

   HP's program til informationssikkerhed er udviklet til at lede og vedligeholde organisationens informationssikkerhedsstrategi og -kontroller. Dette system sikrer, at alle virksomheder overholder HP's sikkerhedspolitikker og -kontrolforanstaltninger samt overholder sine kunders sikkerhedskrav. Den strukturerede tilpasning med branchemæssige cybersikkerhedsstrukturer, love og bestemmelser bliver revideret årligt for at tilpasse den til HP's trusselslandskab, der udvikler sig.

3. Håndtering af risici i forbindelse med cybersikkerhed

   Formålet med HP's program for håndtering af risici i forbindelse med cybersikkerhed er at bevare fortroligheden, integriteten og tilgængeligheden af de tilhørende informationsaktiver. Med programmet får du en konsekvent tilgang til identificering, evaluering, prioritering, behandling, afhjælpning, sporing og rapportering af risici. HP definerer sin risikoappetit som det acceptable niveau for eksponering af tab og risikotolerance som graden af varians i forhold til denne appetit. Risici evalueres vha. en defineret metode, hvilket gør det muligt for HP at nedsætte informationssikkerhedsrisiciene til et acceptabelt niveau. Dette program er i overensstemmelse med HP's Enterprise Risk Management-proces.

4. HR-sikkerhed

   HP's HR-politik sikrer informationssikkerhed gennem hele medarbejderlevecyklussen ved at etablere processer til adgang til faciliteter, informationssystemer og andre aktiver. Det omfatter indhente skriftlige bekræftelser gennem fortrolighedsaftaler og hemmeligholdelsesaftaler samt gennemførelse af baggrundsscreeningsprocedurer. Alle jobsøgende hos HP skal bestå en baggrundsgodkendelse i overensstemmelse med relevante love, bestemmelser og etik.

5. Administration af aktiv

   HP har en proces til identifikation af tekniske aktivoplysninger, kategorisering af kritiske aktiver og vedligeholdelse af dokumenterede håndteringsprocedurer for hver enkelt klassificeringstype, herunder dem der indeholder personlige data. Disse procedurer omfatter opbevaring, transmission, kommunikation, adgang, logging, tilbageholdelse, ødelæggelse, bortskaffelse, hændelsesadministration og meddelelse om brud. HP's sikkerhedspolitikker og -standarder bemyndiger også sikker bortskaffelse af medier.

6. Datasikkerhed

   HP's datasikkerhedsprogram beskriver den sikkerhedspraksis og de tekniske kontrolforanstaltninger, der skal implementeres for at beskytte fortroligheden, autenciteten og dataintegriteten. Juridiske krav, værdi, kritiskhed og følsomhed for uautoriseret offentliggørelse eller ændring er et par af de faktorer, som bestemmer, hvordan oplysningerne klassificeres under HP's datasikkerhedspolitik. Ud over datahåndteringsprocedurer beskriver politikken datakryptering, sletning, indsamling og behandling, opbevaring, backup og forebyggelse af datatab.

7. Adgangskontrol

   HP benytter princippet om mindst privilegium til logisk adgangskontrol og giver brugeradgang gennem unikke bruger-id'er og adgangskoder. Adgangskodepolitikken definerer kompleksiteten, styrken, gyldigheden og adgangskodehistorikken. Adgangsrettighederne gennemgås og ophæves regelmæssigt, når medarbejderne forlader virksomheden. De procedurer, der er aftalt for oprettelse og sletning af brugerkonti, implementeres for at tildele og tilbagekalde adgang til klientsystemer under handlinger.

8. Kryptografi

   HP har defineret et sæt robuste processer til kryptografi, som sikrer fortrolighed, integritet og tilgængelighed af oplysningsaktiver. Godkendte protokoller kræver kryptering af visse aktiver, herunder dem, der indeholder personlige data. Vores kryptografiprogram omfatter brug af matematiske teknikker til sikker information og kommunikation, hvilket sikrer, at kun godkendte parter har adgang til dataene. En kritisk komponent i HP's informationssikkerhedsprogram beskytter data mod uautoriseret adgang og uautoriserede ændringer.

9. Fysisk og miljømæssig sikkerhed

   HP-faciliteter er sikrede ved brug af forskellige fysiske og elektroniske adgangskontroller, herunder sikkerhedsvagter, elektronisk adgangskontrol og internt tv (CCTV). Faciliteterne er også udstyret med nødvendig infrastruktursupport, herunder temperaturstyring og strøm-backup, ved brug af UPS og/eller dieselgeneratorer til understøttelse af kritiske tjenester. Alle HP-medarbejdere er registreret og skal bære relevante identifikationsbadges.

10. Administration af drift

    HP har etableret minimumskrav til styrkelses af teknologiinfrastruktur, herunder arbejdsstationer, servere og netværksudstyr. Disse enheder bruger forudstyrkede operativsystembilleder med forskellige krav til operativsystemet og implementerede kontrolforanstaltninger. Derudover har HP implementeret NIDS/NIPS (Network Intrusion Detection/Prevention Systems), som overvåges og administreres 24/7.

11. Kommunikationssikkerhed

    Kommunikationssikkerhed sikrer beskyttelse af oplysninger i virksomhedsnetværk. Det omfatter installation og administration af netværkssikkerhedskomponenter (f.eks. firewalls), adskillelse af netværk samt webfiltrering og kontrol af e-mailhåndtering. Desuden omfatter det overvågning og administration af kommunikationskanaler for at registrere og forhindre uautoriseret adgang eller databrud.

12. Systemsikkerhed

    HP's politik bemyndiger en sikker udviklingsmetode for systemer og software i hele deres levetid. Software Development Lifecycle dækker opstart, udvikling/ erhvervelse, implementering, drift og bortskaffelse. Alle systemkomponenter evalueres for deres indvirkning på den generelle sikkerhed. HP har etableret kontrolforanstaltninger for applikationstjenestetransaktioner, herunder godkendelse af brugerlegitimationsoplysninger, digitale signaturer, kryptering, sikre kommunikationsprotokoller og lagring af transaktionsoplysninger i den relevante netværkssikkerhedszone. Der udføres også regelmæssige interne scanninger af sårbarheder.

13. Tredjeparter og underleverandører

    HP har processer til at vælge underentreprenører, som overholder omfattende kontraktmæssige sikkerhedskrav. For de gældende leverandører, der håndterer HP- eller kundedata eller får adgang til HP-netværket, udfører HP Cybersecurity en risikovurdering for at kontrollere et informationssikkerhedsprogram med fysiske, tekniske og administrative sikkerhedsforanstaltninger. Denne vurdering er påkrævet, før leverandøren kan få adgang til HP-oplysninger.

14. Administration af sikkerhedshændelser i forbindelse med oplysninger

    HP har en omfattende cyber-hændelsesadministrationsproces, som beskriver formål, omfang, roller, ansvar, administrationsforpligtelse, organisatorisk koordination, implementeringsprocedurer og kontrol af overholdelse. Denne proces gennemgås og opdateres årligt. Cyber-hændelsessvarteamet, herunder HP Cybersecurity-medarbejdere, der er uddannet i hændelsesbesvaring og krisestyring, udfører regelmæssige tabel-top-anmeldelser af processen og eventuelle hændelser eller begivenheder.

15. Styring af virksomhedskontinuitet

    HP's globale Continuity of Operations-program sikrer komplet kontinuitet gennem samarbejdsbaserede, standardiserede og dokumenterede planlægningsprocesser. Virksomheden benytter regelmæssigt deres forretningskontiunitetsplaner for at sikre effektivitet, test og opdatering af alle planer mindst én gang om året. Desuden modtager alt personale, der er involveret i virksomhedens kontinuitetsplan, korrekt uddannelse.

16. Overholdelse.

    Overholdelse former HP's tilgang til at opfylde juridiske, kontraktlige og interne forventninger til et effektivt oplysningssikkerhedsprogram. Regelmæssige informationssikkerhedsanmeldelser sikrer, at protokoller er integreret i hver forretningsgruppes handlinger. Revisionsprocessen holder også dokumenter opdateret, så de afspejler de nuværende juridiske forpligtelser i takt med, at kravene udvikler sig.

17. Payment Card Industry

    PCI-strukturen (Payment Card Industry) guider HP's fremgangsmpde med at nå PCI-overholdelse og beskriver de forretningsansvar og sikkerhedskontroller, der er justeret i forhold til PCI DSS. Ved at installere og vedligeholde netværkssikkerhedskontroller, som f.eks. firewalls, sikrer HP, at den opfylder PCI-overholdelseskravene.

18. HP-produktsikkerhed

    HP-produktsikkerhed omfatter grundlæggende praksis for at sikre HP-produkter, f.eks. kodesignering, administration af produktsikkerhedssvagheder, udstedelse af sikkerhedsbulletiner og rapportering af produktsikkerhedsproblemer. Disse tiltag sikrer, at HP-produkterne forbliver sikre og pålidelige for brugerne. Produktsikkerhed er centralt for HP, da det hjælper med at opretholde kundetillid og beskytter mod potentielle trusler.

19. HP Service Security

    HP Service Security omfatter grundlæggende praksis for at sikre de tjenester, der leveres til HP-kunder. Denne politik behandler forskellige områder inden for servicesikkerhed, herunder HP-infrastrukturvært, hostede tredjepartsværter, partnerværter og brugerværtsmiljøer. Disse foranstaltninger sikrer, at HP-tjenester forbliver sikre og pålidelige for brugerne. Ved at implementere robust sikkerhedspraksis sikrer HP sikkerheden og integriteten af sine produkter og tjenester og skaber et sikkert og troværdigt miljø for alle brugere.