SAMMENDRAG AV HPS SIKKERHETSTILTAK

For å beskytte kundedataene har HP implementert strenge informasjonssikkerhetskontroller, herunder policyer, rutiner, prosedyrer og organisasjonsstrukturer, som skal ivareta konfidensialiteten, integriteten og tilgangen til selskapets og kundenes informasjon (innbefattet personopplysninger, som definert i HPs tillegg om kunde- og databehandling). Under finner du en oversikt over de tekniske/organisatoriske sikkerhetstiltakene som er implementert overalt hos HP.

1. Sikkerhetspolicy

   HP har implementert globale policyer, standarder og prosedyrer som skal beskytte HP- og kundedata. For å verne om integriteten til HPs data og systemer er detaljene i HPs sikkerhetspolicyer konfidensielle. Du finner imidlertid et sammendrag av de sentrale policyene våre under.

2. Informasjonssikkerhetsorganisasjon

   Hensikten med HPs program for informasjonssikkerhet er å styre og ajourføre organisasjonens strategi og kontroller for informasjonssikkerhet. Dette systemet sørger for at HPs sikkerhetspolicyer og kontroller følges overalt i virksomheten, og at kundenes sikkerhetskrav innfris. Rammeverket er strukturert i samsvar med lover og forskrifter samt standard bransjerammeverk for cybersikkerhet, og evalueres og oppdateres årlig ut fra endringer i HPs trussellandskap.

3. Behandling av cybersikkerhetsrisiko

   HPs program for behandling av cybersikkerhetsrisiko er utformet for å beskytte konfidensialiteten, integriteten og tilgangen til informasjonsressurser. Programmet sørger for en konsekvent tilnærming med hensyn til identifisering, vurdering, prioritering, behandling, utbedring, sporing og rapportering av cybersikkerhetsrisikoer. HP definerer sin risikoappetitt som et akseptabelt nivå av eksponering for tap, og risikotoleranse som graden av avvik fra denne appetitten. Risikoer evalueres ved hjelp av en definert metodologi som gjør det mulig for HP å redusere informasjonssikkerhetsrisikoene til et akseptabelt nivå. Dette programmet er samkjørt med HPs prosess for behandling av virksomhetsrisiko.

4. HR-sikkerhet

   HPs policy for HR-sikkerhet ivaretar informasjonssikkerheten gjennom hele livssyklusen til medarbeiderne ved å etablere prosesser for tilgang til fasiliteter, informasjonssystemer og andre ressurser. Dette innbefatter innhenting av skriftlige bekreftelser gjennom konfidensialitets- og ikke-avsløringsavtaler, samt screening av bakgrunn. Alle som søker jobb hos HP, må gjennom en bakgrunnskontroll i samsvar med relevante lover, forskrifter og etiske retningslinjer.

5. Ressursforvaltning

   HP har en prosess for identifisering av tekniske informasjonsressurser, kategorisering av kritiske ressurser og ajourføring av dokumenterte behandlingsprosedyrer for hver informasjonsklasse, innbefattet informasjonsklasser som inneholder personopplysninger. Disse prosedyrene omfatter lagring, overføring, kommunikasjon, tilgang, loggføring, oppbevaring, destruksjon, sletting, behandling av hendelser og varsel om brudd. HPs sikkerhetspolicyer og standarder krever i tillegg sikker avhending av medier.

6. Datasikkerhet

   HPs datasikkerhetsprogram beskriver sikkerhetsrutinene og de tekniske kontrollene som må implementeres for å ivareta konfidensialiteten, autentisiteten og integriteten til dataene. Juridiske krav, verdi, kritisk betydning og sensitivitet for uautorisert avsløring eller modifisering er blant faktorene som avgjør hvordan informasjon klassifiseres etter HPs policy for datasikkerhet. I policyen beskrives prosedyrene for håndtering av data, datakryptering, sletting, innsamling, behandling, oppbevaring, sikkerhetskopiering og forebygging av datatap.

7. Tilgangskontroll

   HP bruker prinsippet om minste privilegium for logisk tilgangskontroll, og gir brukertilgang gjennom unike bruker-ID-er og passord. I passordpolicyen defineres kompleksitet, styrke, gyldighet og kontroller for passordhistorikk. Tilgangsrettighetene gås gjennom med jevne mellomrom og tilbakekalles ved avslutning av arbeidsforhold. Avtalte prosedyrer for oppretting og sletting av brukerkontoer implementeres for å innvilge og tilbakekalle tilgang til klientsystemer i forbindelse med oppdrag.

8. Kryptografi

   HP har definert et sett med solide prosesser for kryptografi for å sikre konfidensialitet, integritet og tilgjengelighet for informasjonsressurser. Godkjente protokoller krever kryptering av bestemte ressurser, herunder ressurser som inneholder personopplysninger. I kryptografiprogrammet vårt benyttes matematiske teknologier for å sikre informasjon og kommunikasjon, slik at kun autoriserte parter har datatilgang. En kritisk komponent i HPs program for informasjonssikkerhet er beskyttelse av data mot uautorisert tilgang og manipulering.

9. Fysisk og miljømessig sikkerhet

   HPs fasiliteter er sikret gjennom ulike fysiske og elektroniske tilgangskontroller, innbefattet sikkerhetsvakter, elektronisk tilgangskontroll og kameraovervåkning (CCTV). Fasilitetene er i tillegg utstyrt med nødvendig støtteinfrastruktur, herunder temperaturkontroll og nødstrøm gjennom avbruddsfrie strømforsyninger (UPS) og/eller dieselgeneratorer, for å sikre kritiske tjenester. Alt HP-personell er registrert og plikter å bære identifikasjon.

10. Operasjonsbehandling

    HP har etablerte minstekrav til herding av teknologiinfrastruktur, innbefattet arbeidsstasjoner, servere og nettverksutstyr. Disse enhetene bruker forhåndsherdede operativsystembilder, der kravene varierer alt etter operativsystem og implementerte kontroller. I tillegg har HP distribuert NIDS/NIPS-systemer (Network Intrusion Detection/Prevention Systems) som overvåkes og administreres døgnet rundt.

11. Kommunikasjonssikkerhet

    Kommunikasjonssikkerheten sørger for at informasjonen i konsernnettverk beskyttes. Dette omfatter installering og administrering av nettverkssikkerhetskomponenter (f.eks. brannmurer), adskillelse av nettverk samt nettfiltrering og kontroller for håndtering av e-post. I tillegg overvåkes og administreres kommunikasjonskanaler for å fange opp og forebygge uautorisert tilgang eller databrudd.

12. Systemsikkerhet

    HPs policyer krever en sikker utviklingsmetodologi for systemer og programvare hele livssyklusen igjennom. Livssyklusen for programvareutvikling omfatter initiering, utvikling/anskaffelse, implementering, drift og avhending. Samtlige systemkomponenter evalueres ut fra hvordan de påvirker den samlede sikkerheten. HP har implementert kontroller for tjenestetransaksjoner, herunder validering av påloggingsinformasjon for brukere, digitale signaturer, kryptering, sikre kommunikasjonsprotokoller og lagring av transaksjonsdetaljer i riktig sikkerhetssone i nettverket. I tillegg gjennomføres jevnlige skanninger for å identifisere eventuelle interne sårbarheter.

13. Tredjeparter og underleverandører

    HP har prosesser for å velge ut underleverandører som innfrir omfattende kontraktfestede sikkerhetskrav. For leverandører som håndterer HP- eller kundedata, eller som har tilgang til HP-nettverket, utfører HPs ansvarlige for cybersikkerhet en risikovurdering for å bekrefte at det brukes et program for informasjonssikkerhet som omfatter fysiske, tekniske og administrative sikkerhetstiltak. Denne vurderingen kreves utført før leverandøren får tilgang til HP-informasjon.

14. Behandling av informasjonssikkerhetshendelser

    HP har en omfattende prosess for behandling av cyberhendelser. Her skisseres formål, omfang, roller, ansvar, ledelsesansvar, organisatorisk koordinering, implementeringsprosedyrer og kontroll av etterlevelse. Denne prosessen blir gått gjennom og oppdatert årlig. Responsteamet for cyberhendelser, innbefattet HP-cybersikkerhetspersonale som har fått opplæring i hendelses- og krisehåndtering, utfører jevnlige gjennomganger av prosessen og eventuelle hendelser.

15. Forretningskontinuitetsstyring

    HPs globale program for driftskontinuitet sikrer ende-til-ende-kontinuitet gjennom standardiserte, dokumenterte og samarbeidsbaserte planleggingsprosesser. Selskapet følger opp at planene for forretningskontinuitet fungerer effektivt, og tester og oppdaterer samtlige planer minst én gang i året. I tillegg sørges det for relevant opplæring til alt personell som er involvert i planene for forretningskontinuitet.

16. Etterlevelse (compliance)

    HPs tilnærming til juridiske, kontraktfestede og interne forventninger til et effektivt program for informasjonssikkerhet følger kravene om etterlevelse. Jevnlige evalueringer av informasjonssikkerheten sørger for at protokoller er integrert i alle deler av selskapets driftsvirksomhet. I evalueringsprosessen oppdateres samtidig dokumentene slik at de speiler de til enhver tid gjeldende juridiske forpliktelsene.

17. Payment Card Industry

    HP følger PCI-rammeverket (Payment Card Industry) og har definert virksomhetsansvar og implementert sikkerhetskontroller i samsvar med PCI DSS. Ved å installere og vedlikeholde nettverkssikkerhetskontroller i form av bl.a. brannmurer sørger HP for at kravene til PCI-etterlevelse innfris.

18. HP-produktsikkerhet

    HP-produktsikkerheten omfatter viktige rutiner for å sikre HP-produkter, herunder kodesignering, administrering av sårbarheter i produktsikkerheten, utstedelse av sikkerhetsoppslag og rapportering av problemer knyttet til produktsikkerheten. Disse tiltakene sørger for at HP-produktene fortsetter å være sikre og pålitelige for brukerne. Produktsikkerheten er av største betydning for HP – både for å bevare kundenes tillit og for å forebygge potensielle trusler.

19. HP-tjenestesikkerhet

    HP-tjenestesikkerheten omfatter viktige rutiner for å sikre tjenestene som HP leverer til kundene sine. Denne policyen omhandler ulike områder av tjenestesikkerheten, herunder driftede miljøer i HP-infrastrukturen, hos tredjeparter, samarbeidspartnere og kunder. Disse tiltakene sørger for at HP-tjenestene fortsetter å være sikre og pålitelige for brukerne. Gjennom implementering av robuste sikkerhetsrutiner ivaretar HP sikkerheten og integriteten til selskapets produkter og tjenester, og tilrettelegger for et sikkert og pålitelig miljø for samtlige brukere.