YHTEENVETO HP:N TIETOTURVATOIMISTA

HP suojaa asiakastiedot käyttämällä tehokkaita tietoturvan valvontakeinoja, kuten käytäntöjä, menettelyitä ja organisaatiorakenteita, omien ja asiakkaidensa tietojen (mukaan lukien HP:n asiakas- ja tietojenkäsittelyliitteissä määritetyt henkilötiedot) luottamuksellisuuden, eheyden ja saatavuuden suojaamiseksi. Seuraavassa on yleiskuvaus HP:n teknisistä / organisaatioon liittyvistä tietoturvatoimista koko yrityksessä.

1. Suojauskäytäntö

   HP ylläpitää maailmanlaajuisesti sovellettavia käytäntöjä, standardeja ja menettelyitä, jotka on tarkoitettu suojaamaan HP:n ja asiakkaiden tietoja. HP:n suojauskäytäntöjen yksityiskohdat ovat luottamuksellisia HP:n tietojen ja järjestelmien eheyden suojaamiseksi. Seuraavassa on kuitenkin yhteenveto keskeisistä käytännöistämme.

2. Tietoturvaorganisaatio

   HP:n tietoturvaohjelma on suunniteltu ohjaamaan ja ylläpitämään organisaation tietoturvastrategiaa ja valvontakeinoja. Tämä järjestelmä varmistaa koko yrityksessä HP:n suojauskäytäntöjen ja valvontakeinojen sekä asiakkaiden suojausvaatimusten noudattamisen. Kehys vastaa alan vakiona olevia kyberturvallisuuskehyksiä, lakeja ja määräyksiä, ja sitä tarkistetaan vuosittain HP:n muuttuvan uhkaympäristön mukaan.

3. Kyberturvallisuusriskien hallinta

   HP:n kyberturvallisuusriskien hallintaohjelma on suunniteltu säilyttämään luottamuksellisuus, eheys ja tietoresurssien saatavuus. Ohjelmassa on johdonmukainen lähestymistapa kyberturvallisuusriskien tunnistamiseen, arviointiin, priorisointiin, käsittelyyn, korjaamiseen, seurantaan ja raportointiin. HP määrittelee riskinottohalukkuutensa hyväksyttäväksi altistumisen tasoksi ja riskitoleranssin tästä aiheutuvan vaihtelun asteeksi. Riskejä arvioidaan käyttämällä määritettyä menetelmää, jonka avulla HP voi alentaa tietoturvariskit hyväksyttävälle tasolle. Ohjelma on linjassa HP:n Enterprise Risk Management -prosessin kanssa.

4. Henkilöstöhallinnon suojaus

   HP:n henkilöstöhallinnon suojauskäytännöllä varmistetaan tietoturva työntekijöiden koko työsuhteen ajan määrittämällä tiloja, tietojärjestelmiä ja muita resursseja koskevia käyttöoikeusprosesseja. Tähän sisältyy kirjallisten hyväksyntöjen hankinta luottamuksellisuus- ja salassapitosopimusten avulla sekä taustaseulontamenettelyjen käyttö. Kaikkien HP:ltä työtä hakevien on käytävä läpi taustatarkistus asianmukaisten lakien, säännösten ja eettisten periaatteiden mukaisesti.

5. Resurssien hallinta

   HP:llä on prosessi, jolla tunnistetaan tekniset tietoresurssit, luokitellaan kriittiset resurssit ja ylläpidetään kunkin tietoluokitustyypin dokumentoituja käsittelymenettelyitä, mukaan lukien henkilötietoja sisältävät resurssit. Nämä menettelyt kattavat varastoinnin, lähetyksen, tiedonsiirron, pääsyn, kirjauksen, säilytyksen, tuhoamisen, hävittämisen, tapahtumien hallinnan ja rikkomusilmoitukset. HP:n suojauskäytännössä ja -standardeissa määrätään myös tietovälineiden turvallisesta hävittämisestä.

6. TIETOTURVA

   HP:n tietoturvaohjelmassa kuvataan suojauskäytännöt ja tekniset keinot, jotka on otettava käyttöön tietojen luottamuksellisuuden, aitouden ja eheyden varmistamiseksi. Lakisääteiset vaatimukset, arvo, kriittisyys ja altistuminen luvattomalle julkistamiselle tai muuttamiselle ovat tekijöitä, jotka määrittävät tietojen luokittelutavan HP:n tietoturvakäytännön perusteella. Tietojenkäsittelymenetelmien lisäksi käytännössä kuvataan tietojen salaus, poistaminen, keräys ja käsittely, säilytys, varmuuskopiointi ja tietojen menetyksen estäminen.

7. Käyttöoikeuksien hallinta

   HP soveltaa loogiseen käyttöoikeuksien hallintaan vähäisimpien oikeuksien periaatetta ja mahdollistaa käytön yksilöivillä käyttäjätunnuksilla ja salasanoilla. Salasanakäytäntö määrittää monimutkaisuuden, vahvuuden, kelvollisuuden ja salasanahistorian asetukset. Käyttöoikeudet tarkistetaan säännöllisin väliajoin ja ne poistetaan työntekijöiden lähdettyä yrityksestä. Käyttäjätilien luonnissa ja poistossa käytettäviä sovittuja menettelyjä sovelletaan myönnettäessä ja evättäessä asiakasjärjestelmien käyttöoikeuksia sitoumusten aikana.

8. Salaus

   HP on määrittänyt tehokkaita salausprosesseja, jotka varmistavat tietoresurssien luottamuksellisuuden, eheyden ja saatavuuden. Hyväksytyt yhteyskäytännöt edellyttävät tiettyjen, myös henkilötietoja sisältävien, resurssien salausta. Salausohjelmassamme hyödynnetään matemaattisia tekniikoita tietojen ja viestinnän suojaamiseksi sekä sen varmistamiseksi, että vain valtuutetut tahot voivat käyttää tietoja. Olennainen osa HP:n tietoturvaohjelmaa on tietojen suojaus luvattomalta käytöltä ja peukaloinnilta.

9. Fyysinen ja ympäristön turvallisuus

   HP:n tiloja suojataan käyttämällä erilaisia fyysisiä ja elektronisia kulunvalvontakeinoja, kuten vartijoita, elektronista kulunvalvontaa ja videovalvontajärjestelmiä (CCTV). Tiloissa on myös tarvittavan infrastruktuurin tuki, mukaan lukien lämpötilan säätö ja varavirtalähteet, joka toteutetaan UPS- ja/tai dieselgeneraattoreilla kriittisten palvelujen varmistamiseksi. Kaikki HP:n työntekijät on rekisteröity, ja heillä on asianmukaiset kulkuluvat.

10. Toimintojen hallinta

    HP on määrittänyt suojauksen vähimmäisvaatimukset tekniselle infrastruktuurille, kuten työasemille, palvelimille ja verkkolaitteille. Näissä laitteissa käytetään valmiiksi suojattuja käyttöjärjestelmän näköiskopioita, joiden vaatimukset vaihtelevat käyttöjärjestelmän ja käytettävien ohjausobjektien mukaan. Lisäksi HP on ottanut käyttöön NIDS (Network Intrusion Detection/Prevention Systems) -järjestelmiä, joita valvotaan ja hallitaan joka päivä ympäri vuorokauden.

11. Tietoliikenteen suojaus

    Tietoliikenteen suojaus turvaa yritysverkkojen tietoja. Näihin järjestelmiin kuuluvat verkon suojauskomponenttien (esim. palomuurien) asennus ja hallinta, verkkojen eriyttäminen sekä web-suodatuksen ja sähköpostin käsittelyn toiminnot. Lisäksi niihin sisältyvät tiedonsiirtokanavien valvonta ja hallinta luvattoman käytön ja tietomurtojen estämiseksi.

12. Järjestelmien suojaus

    HP:n käytännön mukaan järjestelmiä ja ohjelmistoja täytyy kehittää turvallisesti niiden koko elinkaaren ajan. Ohjelmistokehityksen elinkaari kattaa aloittamisen, kehityksen/hankinnan, käyttöönoton, käytön ja hävittämisen. Kaikki järjestelmäkomponentit arvioidaan sen kannalta, miten ne vaikuttavat yleiseen suojaustasoon. HP on määrittänyt sovelluspalvelutapahtumia varten valvontakeinoja, kuten käyttäjätietojen tarkistuksen, digitaaliset allekirjoitukset, salauksen, suojatut tietoliikenneprotokollat sekä tapahtumatietojen tallennuksen asianmukaiselle verkkosuojausvyöhykkeelle. Sisäisiä haavoittuvuustarkistuksia suoritetaan myös säännöllisesti.

13. Kolmannet osapuolet ja alihankkijat

    HP:llä on prosesseja, joilla valitaan kattavien sopimusperusteisten suojausvaatimusten mukaisia alihankkijoita. HP:n tai asiakkaan tietoja käsitteleville tai HP:n verkkoon pääseville toimittajille HP:n kyberturvallisuusyksikkö tekee riskinarvioinnin vahvistaakseen tietoturvaohjelmaa fyysisillä, teknisillä ja hallinnollisilla suojaustoimilla. Tämä arviointi on suoritettava, ennen kuin toimittaja voi käyttää HP:n tietoja.

14. Tietoturvahäiriöiden hallinta

    HP:llä on kattava kyberhäiriöiden hallintaprosessi, jossa kuvataan tarkoitus, laajuus, roolit, vastuut, johdon sitoumus, koordinointi organisaatiossa, käyttöönottomenettelyt ja vaatimustenmukaisuuden tarkistus. Tätä prosessia tarkastellaan ja päivitetään vuosittain. Kybertapahtumien toimintatiimi, johon kuuluu häiriöihin reagointia ja kriisinhallintaa varten koulutettu HP:n kyberturvallisuushenkilöstö, arvioi säännöllisissä harjoituksissa prosessia ja mahdollisia häiriöitä tai virhetilanteita.

15. Liiketoiminnan jatkuvuuden hallinta

    HP:n maailmanlaajuisessa toiminnan jatkuvuusohjelmassa varmistetaan päästä päähän -jatkuvuus käyttämällä yhteistyömuotoisia, standardoituja ja dokumentoituja suunnitteluprosesseja. Yhtiö käy jatkuvuussuunnitelmiaan säännöllisesti läpi tehokkuuden, testauksen ja päivityksen varmistamiseksi vähintään vuosittain. Lisäksi kaikki liiketoiminnan jatkuvuussuunnitelmaan osallistuvat työntekijät saavat asianmukaista koulutusta.

16. Vaatimustenmukaisuus

    Vaatimustenmukaisuus muovaa HP:n tapaa täyttää oikeudelliset, sopimusperusteiset ja sisäiset odotukset tehokkaasta tietoturvaohjelmasta. Tietoturvan säännöllisen tarkastelun avulla varmistetaan, että protokollat on integroitu kunkin liiketoimintaryhmän toimintoihin. Tarkistusprosessissa asiakirjat myös päivitetään vastaamaan nykyisiä oikeudellisia velvoitteita vaatimusten muuttuessa.

17. Maksukorttiala

    PCI (Payment Card Industry) -kehys ohjaa HP:n lähestymistapaa PCI-vaatimustenmukaisuuden saavuttamisessa sekä linjaa PCI DSS -standardin mukaisia vastuualueita ja suojaustoimia. Kun HP asentaa ja ylläpitää verkon suojaustoimia, kuten palomuureja, se varmistaa täyttävänsä vaatimustenmukaisuutta koskevat PCI-vaatimukset.

18. HP:n tuotteiden suojaus

    HP:n tuotesuojaus kattaa keskeiset käytännöt HP:n tuotteiden suojaamiseksi, kuten koodin allekirjoituksen, tuotteen tietoturvahaavoittuvuuksien hallinnan, tietoturvatiedotteiden antamisen ja raportoinnin tuotteen suojausongelmista. Näillä toimenpiteillä varmistetaan, että HP:n tuotteet pysyvät turvallisina ja luotettavina käyttäjien kannalta. Tuotteiden suojaus on erittäin tärkeää HP:lle, sillä se auttaa säilyttämään asiakkaiden luottamuksen ja antaa suojaa mahdollisia uhkia vastaan.

19. HP:n palvelujen suojaus

    HP:n palvelusuojaus käsittää keskeiset käytännöt HP:n asiakkaille tarjoamien palvelujen suojaamisessa. Tämä käytäntö koskee palvelusuojauksen eri alueita, kuten HP:n infrastruktuurin, kolmansien osapuolten, kumppaneiden ja asiakkaiden isännöimiä ympäristöjä. Näillä toimenpiteillä varmistetaan, että HP:n palvelut pysyvät turvallisina ja luotettavina käyttäjien kannalta. Käyttämällä vahvoja suojauskäytäntöjä HP varmistaa tuotteidensa ja palvelujensa turvallisuuden ja eheyden sekä edistää siten turvallista ja luotettavaa ympäristöä kaikille käyttäjille.