ÖVERSIKT ÖVER HP:S SÄKERHETSÅTGÄRDER

FÖR att skydda kunddata väljer HP att utföra en robust uppsättning informationssäkerhetskontroller inklusive policyer, praxis, procedurer och organisationsstrukturer för att skydda sekretess, integritet och tillgänglighet för sin egen och sina kunders information (inklusive Personuppgifter enligt definitionen i HP:s tillägg till kund och databearbetning). Nedan anges en översikt över HP:s tekniska/organisatoriska säkerhetsåtgärder i hela företaget.

1. Säkerhetspolicy

   HP upprätthåller globalt tillämpliga principer, standarder och procedurer avsedda att skydda HP-data och kunddata. Detaljerna i HP:s säkerhetsprinciper är konfidentiella för att skydda integriteten för HP:s data och system. Sammanfattningar av våra viktigaste policyer ingår dock nedan.

2. Organisation för informationssäkerhet

   HP:s informationssäkerhetsprogram är utformat för att styra och underhålla organisationens strategi och kontroller för informationssäkerhet. Det här systemet garanterar att HP:s säkerhetsprinciper och kontroller i hela företaget följs samt att kundernas säkerhetskrav följs. Ramverket är uppbyggt i linje med branschstandardramar för cybersäkerhet, lagar och förordningar och ses över årligen för att anpassa sig till HP:s föränderliga hotlandskap.

3. Hantering av cybersäkerhetsrisker

   HP:s hanteringsprogram för cybersäkerhet är utformat för att bevara sekretess, integritet och tillgång till dess informationstillgångar. Programmet tillhandahåller ett konsekvent tillvägagångssätt för att identifiera, bedöma, prioritera, behandla, åtgärda, spåra och rapportera cybersäkerhetsrisker. HP definierar riskaptiten som den acceptabla förlustexponeringen och risktoleransen som graden av variation från denna aptit. Risker utvärderas med hjälp av en definierad metod, vilket gör det möjligt för HP att reducera informationssäkerhetsriskerna till en acceptabel nivå. Det här programmet överensstämmer med HP:s riskhanteringsprocess för företag.

4. HR-säkerhet

   HP:s policy för personalsäkerhet garanterar informationssäkerhet under hela medarbetarlivscykeln genom att upprätta processer för åtkomst till anläggningar, informationssystem och andra tillgångar. Detta inkluderar att erhålla skriftliga erkännanden via integritets- och sekretessavtal samt att genomföra bakgrundskontroller. Alla som kandiderar till anställning hos HP måste göra en bakgrundskontroll i enlighet med relevanta lagar, förordningar och etik.

5. Kapitalförvaltning

   HP har en process för att identifiera tekniska informationstillgångar, kategorisera kritiska tillgångar och underhålla dokumenterade hanteringsprocedurer för varje typ av informationsklassificering, inklusive de som innehåller personuppgifter. Dessa procedurer omfattar lagring, överföring, kommunikation, åtkomst, loggning, lagring av uppgifter, destruktion, kassering, incidenthantering och underrättelse om brott. HP:s säkerhetsprinciper och standarder kräver också säker kassering av material.

6. Datasäkerhet

   HP:s datasäkerhetsprogram beskriver de säkerhetsåtgärder och tekniska kontroller som måste genomföras för att skydda datas sekretess, äkthet och integritet. Lagkrav, värde, allvarlighet och känslighet för otillåten spridning eller modifiering är några av de faktorer som bestämmer hur information klassificeras enligt HP:s datasäkerhetspolicy. Förutom procedurer för datahantering beskriver principen datakryptering, radering, insamling och bearbetning, lagring av uppgifter, säkerhetskopiering och förebyggande av dataförlust.

7. Åtkomstkontroll

   HP använder principen om minst behörighet för logisk åtkomstkontroll och ger användaråtkomst via unika användar-ID:n och lösenord. Lösenordsprincipen definierar komplexitet, styrka, giltighet och kontroller för lösenordshistorik. Åtkomsträttigheterna ses över och upphävs regelbundet vid uppsägning av personal. Överenskomna procedurer för att skapa och ta bort användarkonton implementeras för att bevilja och återkalla åtkomst till klientsystem under engagemang.

8. Kryptografi

   HP har definierat en uppsättning robusta processer för kryptografi för att säkerställa sekretess, integritet och tillgång till informationstillgångar. Godkända protokoll kräver kryptering för vissa tillgångar, inklusive sådana som innehåller personliga data. Vårt kryptografiprogram innebär användning av matematiska tekniker för att säkra information och kommunikation, vilket säkerställer att endast auktoriserade parter kan få tillgång till uppgifterna. En kritisk komponent i HP:s informationssäkerhetsprogram skyddar data från obehörig åtkomst och manipulation.

9. Fysisk och miljömässig säkerhet

   HP:s anläggningar skyddas med hjälp av olika fysiska och elektroniska åtkomstkontroller, däribland säkerhetsvakter, elektronisk åtkomstkontroll och kameraövervakning (CCTV). Anläggningarna är också utrustade med nödvändigt infrastrukturstöd, inklusive temperaturkontroll och strömbackup, med UPS- och/eller dieselkraftkraftverk för att stödja viktiga tjänster. All HP-personal är registrerad och för att ha lämpliga identifieringsbrickor.

10. Verksamhetshantering

    HP har upprättat minimihärdningskrav för teknikinfrastruktur, inklusive arbetsstationer, servrar och nätverksutrustning. Dessa enheter använder förhärdade bilder av operativsystem, med krav som varierar enligt operativsystemet och implementerade kontroller. HP har dessutom distribuerat NIDS/NIPS (Network Intrusion Detection/Prevention Systems) som övervakas och hanteras 24/7.

11. Kommunikationssäkerhet

    Kommunikationssäkerhet garanterar informationsskyddet i företagsnätverk. Detta innefattar installation och hantering av nätverkssäkerhetskomponenter (t.ex. brandväggar), segregering av nätverk samt kontroller för webbfiltrering och e-posthantering. Dessutom inkluderar det övervakning och hantering av kommunikationskanaler för att upptäcka och förhindra obehöriga åtkomst- eller dataöverträdelser.

12. Systemsäkerhet

    HP:s policy ger mandat för en säker utvecklingsmetod för system och programvara under hela deras livscykel. Livscykeln för programvaruutveckling omfattar initiering, utveckling/förvärv, implementering, drift och kassering. Alla systemkomponenter utvärderas för deras inverkan på den allmänna säkerheten. HP har upprättat kontroller för transaktioner med programtjänster, inklusive validering av användarautentiseringsuppgifter, digitala signaturer, kryptering, säkra kommunikationsprotokoll och lagring av transaktionsinformation inom lämplig nätverkssäkerhetszon. Regelbundna interna sårbarhetsgenomsökningar utförs också.

13. Tredje part och underleverantörer

    HP har processer att välja underentreprenörer som uppfyller omfattande krav på avtalsenlig säkerhet. För tillämpliga leverantörer som hanterar HP-data eller kunddata, eller får tillgång till HP-nätverket, utför HP Cybersecurity en riskbedömning för att verifiera ett informationssäkerhetsprogram med fysiska, tekniska och administrativa skyddsåtgärder. Den här bedömningen krävs innan leverantören kan komma åt HP-information.

14. Hantering av informationssäkerhetsincidenter

    HP har en omfattande hanteringsprocess för cyberincidenter som beskriver syfte, omfattning, roller, ansvar, ledning engagemang, organisationssamordning, implementeringsprocedurer och efterlevnadskontroll. Den här processen görs om och uppdateras årligen. Cyber Incident Response Team, inklusive HP:s personal för cybersäkerhet som är utbildad i incidentsvar och krishantering, utför regelbundna bordsrecensioner av processen och eventuella incidenter eller händelser.

15. Hantering av verksamhetskontinuitet

    HP:s globala kontinuitetsprogram säkerställer kontinuitet genom gemensamma, standardiserade och dokumenterade planeringsprocesser. Företaget utövar regelbundet sin kontinuitet i verksamheten för att säkerställa effektivitet, testning och uppdatering av alla planer minst ett år. Dessutom får all personal som är involverad i affärskontinuitetsplanen lämplig utbildning.

16. Efterlevnad

    Efterlevnad formar HP:s inställning att uppfylla juridiska, avtalsmässiga och interna förväntningar på ett effektivt informationssäkerhetsprogram. Säkerhetsrecensioner av vanlig information garanterar att protokollen integreras i varje verksamhetsgrupps verksamhet. Granskningsprocessen håller också dokumenten uppdaterade för att återspegla de nuvarande rättsliga skyldigheterna i takt med att kraven utvecklas.

17. Betalkortsindustrin

    PCI-ramverket (Payment Card Industry) vägleder HP:s strategi för att uppnå PCI-efterlevnad, vilket beskriver verksamhetens ansvar och säkerhetskontroller i linje med PCI DSS. Genom att installera och underhålla nätverkssäkerhetskontroller som brandväggar försäkrar HP att det uppfyller PCI-efterlevnadskrav.

18. HP:s produktsäkerhet

    HP:s produktsäkerhet omfattar viktiga metoder för att skydda HP-produkter, såsom kodsignering, hantering av säkerhetsproblem för produktens säkerhet, utfärdande av säkerhetsbulletiner och rapportering av problem med produktsäkerhet. Dessa åtgärder garanterar att HP-produkter förblir säkra och tillförlitliga för användare. Produktsäkerhet är av största vikt på HP eftersom den bidrar till att upprätthålla kundernas förtroende och skyddar mot potentiella hot.

19. HP:s servicesäkerhet

    HP:s servicesäkerhet omfattar grundläggande metoder för att skydda de tjänster som tillhandahålls till HP:s kunder. Denna princip behandlar olika områden av servicesäkerhet, inklusive HP-infrastruktur som är värd för, värdmiljöer för tredje part, värdmiljöer och miljöer som betjänar kunder. Dessa åtgärder garanterar att HP:s tjänster förblir säkra och tillförlitliga för användare. Genom att implementera robusta säkerhetsrutiner garanterar HP säkerheten och integriteten för sina produkter och tjänster och främjar en säker och pålitlig miljö för alla användare.