SAMENVATTING VAN DE BEVEILIGINGSMAATREGELEN VAN HP

HP beschermt klantgegevens door een robuuste reeks beveiligingscontroles uit te voeren van informatie, waaronder beleid, praktijken, procedures en organisatiestructuren om de vertrouwelijkheid, integriteit en beschikbaarheid van de eigen informatie en die van zijn klanten te beschermen (met inbegrip van persoonsgegevens zoals gedefinieerd in de Addenda voor klant en gegevensverwerking van HP). Hieronder volgt een overzicht van de technische/organisatorische beveiligingsmaatregelen van HP in het hele bedrijf.

1. Beveiligingsbeleid

   HP voert wereldwijd toepasselijke beleidsregels, standaarden en procedures uit om gegevens van HP en klanten te beschermen. De details van het beveiligingsbeleid van HP zijn vertrouwelijk om de integriteit van de gegevens en systemen van HP te beschermen. Hieronder worden echter korte overzichten van ons belangrijkste beleid opgenomen.

2. Organisatie voor informatiebeveiliging

   Het informatiebeveiligingsprogramma van HP is ontworpen om de strategie en besturingselementen voor informatiebeveiliging van de organisatie te leiden en onderhouden. Dit systeem zorgt ervoor dat het beveiligingsbeleid en de besturingselementen van HP in de hele onderneming worden nageleefd en dat wordt voldaan aan de beveiligingsvereisten van zijn klanten. Het Framework is gestructureerd op basis van industrienormen, wetten en voorschriften voor cyberbeveiliging en wordt jaarlijks herzien om het aan te passen aan het veranderende dreigingslandschap van HP.

3. Risicobeheer voor cyberbeveiliging

   Het programma van HP voor het beheren van cyberbeveiligingsrisico's is erop gericht de vertrouwelijkheid, integriteit en beschikbaarheid van haar informatiemiddelen te waarborgen. Het programma biedt een consistente aanpak voor het identificeren, beoordelen, prioriteren, behandelen, verhelpen, traceren en rapporteren van cyberbeveiligingsrisico's. HP definieert haar Risicobereidheid als het aanvaardbare niveau van blootstelling aan verliezen en Risicotolerantie als de mate van afwijking van deze bereidheid. Risico's worden geëvalueerd aan de hand van een gedefinieerde methodologie, zodat HP de risico's voor informatiebeveiliging tot een acceptabel niveau kan beperken. Dit programma sluit aan op het Enterprise Risk Management-proces van HP.

4. HR Security

   HP Human Resource Security-beleid zorgt voor informatiebeveiliging gedurende de gehele levenscyclus van de werknemer door processen vast te stellen voor toegang tot faciliteiten, informatiesystemen en andere activa. Dit omvat het verkrijgen van schriftelijke bevestigingen door middel van vertrouwelijkheids- en geheimhoudingsovereenkomsten, evenals het uitvoeren van antecedentenonderzoeken. Alle kandidaten voor een dienstverband bij HP moeten een antecedentenonderzoek ondergaan in overeenstemming met de relevante wet- en regelgeving en ethiek.

5. Apparaatbeheer

   HP beschikt over een proces voor het identificeren van technische informatiemiddelen, het categoriseren van kritieke middelen en het onderhouden van gedocumenteerde verwerkingsprocedures voor elk type informatieclassificatie, inclusief middelen die Persoonsgegevens bevatten. Deze procedures hebben betrekking op opslag, overdracht, communicatie, toegang, registratie, bewaring, vernietiging, verwijdering, incidentbeheer en kennisgeving van schendingen. Het beveiligingsbeleid en de beveiligingsnormen van HP schrijven ook voor dat media veilig moeten worden afgevoerd.

6. Gegevensbeveiliging

   Het programma voor gegevensbeveiliging van HP beschrijft de beveiligingspraktijken en technische controles die moeten worden geïmplementeerd om de vertrouwelijkheid, authenticiteit en integriteit van gegevens te beschermen. Wettelijke vereisten, waarde, kriticiteit en gevoeligheid voor ongeoorloofde openbaarmaking of wijziging zijn enkele van de factoren die bepalen hoe informatie wordt geclassificeerd volgens het gegevensbeveiligingsbeleid van HP. Naast de procedures voor gegevensverwerking beschrijft het beleid het versleutelen, wissen, verzamelen en verwerken en bewaren van gegevens, het maken van back-ups en het voorkomen van gegevensverlies.

7. Toegangsbeheer

   HP past het principe van de minste bevoegdheden toe voor logische toegangscontrole, waarbij gebruikerstoegang wordt verleend via unieke gebruikers-id's en wachtwoorden. Het wachtwoordbeleid definieert complexiteit, sterkte, geldigheid en bedieningselementen voor wachtwoordgeschiedenis. De toegangsrechten worden regelmatig herzien en ingetrokken bij vertrek van personeel. Er worden overeengekomen procedures voor het aanmaken en verwijderen van gebruikersaccounts geïmplementeerd om toegang tot clientsystemen toe te kennen en in te trekken tijdens opdrachten.

8. Cryptografie

   HP heeft een reeks robuuste processen voor cryptografie gedefinieerd om de vertrouwelijkheid, integriteit en beschikbaarheid van informatiemiddelen te waarborgen. Goedgekeurde protocollen vereisen versleuteling voor bepaalde activa, waaronder activa die persoonsgegevens bevatten. Ons cryptografische programma omvat het gebruik van wiskundige technieken om informatie en communicatie te beveiligen, zodat alleen geautoriseerde partijen toegang hebben tot de gegevens. Een essentieel onderdeel van het informatiebeveiligingsprogramma van HP is de bescherming van gegevens tegen ongewenste toegang en manipulatie.

9. Fysieke en milieubeveiliging

   De faciliteiten van HP zijn beveiligd met behulp van verschillende fysieke en elektronische toegangscontroles, waaronder beveiligers, elektronisch toegangsbeheer en gesloten televisiecircuits (CCTV). Verder beschikken de faciliteiten over de nodige infrastructuurondersteuning, zoals temperatuurregeling en back-ups, het gebruik van UPS- en/of dieselgeneratoren ter ondersteuning van kritieke services. Alle medewerkers van HP zijn geregistreerd en zijn verplicht om geschikte identificatiebadges te dragen.

10. Operationeel beheer

    HP heeft minimale verhardingseisen opgesteld voor technologie-infrastructuur, waaronder werkstations, servers en netwerkapparatuur. Deze apparaten maken gebruik van voorgeharde installatiekopieën van het besturingssysteem, met vereisten die variëren per besturingssysteem en geïmplementeerde besturingselementen. Bovendien heeft HP detectie-/preventiesystemen voor netwerkinbraken (NIDS/NIPS) geïmplementeerd die 24/7 worden bewaakt en beheerd.

11. Communicatiebeveiliging

    Communicatiebeveiliging zorgt voor de bescherming van informatie in bedrijfsnetwerken. Dit omvat de installatie en het beheer van netwerkbeveiligingscomponenten (bijv. firewalls), scheiding van netwerken, evenals controle op webfiltering en e-mailverwerking. Daarnaast gaat het om het bewaken en beheren van communicatiekanalen om onbevoegde toegang of datalekken op te sporen en te voorkomen.

12. Systeembeveiliging

    Het beleid van HP schrijft een veilige ontwikkelingsmethodologie voor systemen en software gedurende de gehele levenscyclus voor. De levenscyclus van de softwareontwikkeling omvat initiatie, ontwikkeling/verwerving, implementatie, bewerkingen en verwijdering. Alle systeemcomponenten worden geëvalueerd voor hun effect op de algehele beveiliging. HP heeft controles ingesteld voor applicatieservicetransacties, waaronder validatie van gebruikersreferenties, digitale handtekeningen, versleuteling, veilige communicatieprotocollen en opslag van transactiegegevens binnen de juiste netwerkbeveiligingszone. Er worden ook regelmatig interne kwetsbaarheidsscans uitgevoerd.

13. Derden en onderaannemers

    HP beschikt over processen om onderaannemers te selecteren die voldoen aan uitgebreide contractuele beveiligingseisen. Voor leveranciers die gegevens van HP of klanten verwerken, of toegang hebben tot het HP-netwerk, voert HP Cybersecurity een risicobeoordeling uit om een informatiebeveiligingsprogramma met fysieke, technische en administratieve maatregelen te verifiëren. Deze beoordeling is vereist voordat de leverancier toegang krijgt tot HP-informatie.

14. Incidentbeheer voor informatiebeveiliging

    HP beschikt over een uitgebreid beheerproces voor cyberincidenten waarin het doel, de reikwijdte, de rollen, de verantwoordelijkheden, de betrokkenheid van het management, de organisatorische coördinatie, de implementatieprocedures en de controle op naleving worden beschreven. Dit proces wordt jaarlijks herzien en bijgewerkt. Het Cyber Incident Response Team, dat bestaat uit personeel van HP Cybersecurity dat is opgeleid in incidentrespons en crisisbeheersing, voert regelmatig tafelevaluaties uit van het proces en alle incidenten of gebeurtenissen.

15. Beheer van bedrijfscontinuïteit

    Het wereldwijde Continuity of Operations-programma van HP zorgt voor end-to-endcontinuïteit via samenwerkings-, gestandaardiseerde en gedocumenteerde planningsprocessen. Het bedrijf voert periodiek oefeningen met haar ondernemingscontinuïteitsplannen uit om de effectiviteit te garanderen, en test en actualiseert alle plannen minstens één keer per jaar. Bovendien krijgen alle medewerkers die betrokken zijn bij het bedrijfscontinuïteitsplan de juiste opleiding.

16. Compliance

    Compliance geeft vorm aan de aanpak van HP om te voldoen aan wettelijke, contractuele en interne verwachtingen voor een effectief informatiebeveiligingsprogramma. Regelmatige herzieningen van de informatiebeveiliging zorgen ervoor dat protocollen in de activiteiten van elke bedrijfsgroep worden geïntegreerd. Het herzieningsproces zorgt er ook voor dat de documenten bijgewerkt blijven zodat ze de huidige wettelijke verplichtingen weerspiegelen naarmate de vereisten evolueren.

17. Payment Card Industry

    Het PCI-raamwerk (Payment Card Industry) vormt de leidraad voor de aanpak van HP om PCI-compliance te bereiken en beschrijft zakelijke verantwoordelijkheden en beveiligingscontroles die zijn afgestemd op PCI DSS. Door netwerkbeveiligingscontroles zoals firewalls te installeren en te onderhouden, zorgt HP ervoor dat het voldoet aan de vereisten voor PCI-compliance.

18. HP Product Security

    HP Product Security omvat essentiële praktijken voor het beveiligen van HP-producten, zoals code-ondertekening, beheer van kwetsbaarheden in productbeveiliging, uitgifte van beveiligingsbulletins en rapportage van beveiligingsproblemen met het product. Deze maatregelen zorgen ervoor dat HP-producten veilig en betrouwbaar voor de gebruikers blijven. Productbeveiliging is van het allergrootste belang bij HP, omdat dit helpt het vertrouwen van de klant te behouden en te beschermen tegen mogelijke dreigingen.

19. HP Service Security

    HP Service Security omvat essentiële praktijken voor het beveiligen van de services die aan klanten van HP worden geleverd. Dit beleid heeft betrekking op verschillende gebieden van servicebeveiliging, waaronder door de HP-infrastructuur gehoste omgevingen, door derden gehoste omgevingen, door partners gehoste omgevingen en door klanten gehoste omgevingen. Deze maatregelen zorgen ervoor dat de services van HP veilig en betrouwbaar voor gebruikers blijven. Door robuuste beveiligingspraktijken te implementeren, waarborgt HP de veiligheid en integriteit van zijn producten en services, waardoor een veilige en betrouwbare omgeving voor alle gebruikers wordt bevorderd.