# A HP BIZTONSÁGI INTÉZKEDÉSEINEK ÖSSZEFOGLALÁSA

Az Ügyfelek adatainak védelme érdekében a HP az információbiztonsági ellenőrzések szilárd rendszerét alkalmazza, beleértve a saját és ügyfelei adatainak (beleértve a HP Ügyfél- és adatfeldolgozási kiegészítésében meghatározott Személyes adatokat is) titkosságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló irányelveket, gyakorlatokat, eljárásokat és szervezeti struktúrákat. Az alábbiakban áttekintést nyújtunk a HP egész vállalatra kiterjedő műszaki/szervezeti biztonsági intézkedéseiről.

1. Biztonsági szabályzat

   A HP globálisan alkalmazandó irányelveket, szabványokat és eljárásokat tart fenn, amelyek célja a HP és az ügyfelek adatainak védelme. A HP biztonsági irányelveinek részletei titkosak a HP adatai és rendszerei sértetlenségének védelme érdekében. Azonban főbb irányelveink összefoglalása az alábbiakban olvasható.

2. Információbiztonsági szervezet

   A HP Információbiztonsági programjának célja a szervezet információbiztonsági stratégiájának és ellenőrzéseinek irányítása és fenntartása. Ez a rendszer biztosítja az egész vállalatra vonatkozóan a HP biztonsági irányelveinek és ellenőrzéseinek való megfelelést, valamint az ügyfelekkel kapcsolatos biztonsági követelményeknek való megfelelést. Az iparági szabványos kiberbiztonsági keretrendszerekkel, törvényekkel és szabályozásokkal összhangban felépített Keretrendszert évente felülvizsgáljuk, hogy igazodjon a HP-t körülvevő egyre nagyobb fenyegetettséget jelentő környezethez.

3. Kiberbiztonsági kockázatkezelés

   A HP kiberbiztonsági kockázatkezelési programjának célja, hogy megőrizze az információs eszközei titkosságát, sértetlenségét és rendelkezésre állását. A program konzisztens megközelítést alkalmaz a kiberbiztonsági kockázatok azonosítása, felmérése, rangsorolása, kezelése, orvoslása, nyomon követése és jelentése során. A HP a kockázatvállalási hajlandóságot a veszteségnek való kitettség elfogadható szintjeként, a kockázattűrést pedig a hajlandóságtól való eltérés mértékeként határozza meg. A kockázatokat egy meghatározott módszertan alkalmazásával értékeljük ki, amely lehetővé teszi a HP számára az információbiztonsági kockázatok elfogadható szintre történő mérséklését. Ez a program összhangban van a HP Vállalati kockázatkezelési folyamattal.

4. HR Biztonság

   A HP Humán erőforrásra vonatkozó biztonsági irányelve az alkalmazottak teljes életciklusa során biztosítja az információbiztonságot, mert létrehoznak egy, a létesítményekhez, információs rendszerekhez és más eszközökhöz való hozzáférésre szolgáló folyamatokat. Magában foglalja az adatvédelmi és titoktartási megállapodások révén az írásbeli elismeréseket, valamint háttérvizsgálatok elvégzését. A HP-nál történő foglalkoztatásra jelentkező valamennyi jelöltnek a vonatkozó törvényeknek, rendeleteknek és etikai szabályoknak megfelelően át kell esnie a háttérellenőrzésen.

5. Eszközkezelés

   A HP rendelkezik egy eljárással a technikai információs eszközök azonosítására, a kritikus eszközök kategorizálására és a dokumentált kezelési eljárások fenntartására minden egyes információosztályozási típusra vonatkozóan, beleértve a Személyes adatokat tartalmazó eszközöket is. Ezek az eljárások kiterjednek a tárolásra, továbbításra, kommunikációra, hozzáférésre, naplózásra, megőrzésre, megsemmisítésre, ártalmatlanításra, incidenskezelésre és a jogsértések bejelentésére. A HP biztonsági irányelvei és szabványai az adathordozók biztonságos megsemmisítését is előírják.

6. Adatbiztonság

   A HP Adatbiztonsági programja meghatározza azokat a biztonsági gyakorlatokat és technikai ellenőrzéseket, amelyeket az adatok bizalmasságának, hitelességének és sértetlenségének védelme érdekében meg kell valósítani. A jogi követelmények, az érték, a kritikusság és a jogosulatlan nyilvánosságra hozatalra vagy módosításra való érzékenység csak néhány olyan tényező, amely meghatározza, hogy a HP adatbiztonsági irányelvei szerint hogyan osztályozzuk az információkat. Az adatkezelési eljárások mellett az irányelv ismerteti az adatok titkosítását, törlését, gyűjtését és feldolgozását, megőrzését, biztonsági mentését és az adatvesztés megelőzését.

7. Hozzáférés szabályozása

   A HP a legkisebb jogosultság elvét alkalmazza a logikai hozzáférés-szabályozásban, a felhasználók hozzáférését egyedi felhasználói azonosítókkal és jelszavakkal biztosítja. A jelszavakra vonatkozó irányelv meghatározza az összetettség, az erősség, az érvényesség és a jelszó-előzmények ellenőrzését. A hozzáférési jogokat rendszeresen felülvizsgáljuk, és az adott munkatárs távozásakor visszavonjuk. A felhasználói fiókok létrehozására és törlésére vonatkozóan egyeztetett eljárásokat alkalmazunk az ügyfélrendszerekhez való hozzáférés engedélyezésére és visszavonására a megbízások során.

8. Titkosítás

   A HP megbízható kriptográfiai folyamatokat határozott meg az információs eszközök titkosságának, sértetlenségének és rendelkezésre állásának biztosítása érdekében. A jóváhagyott protokollok bizonyos eszközök, köztük a személyes adatokat tartalmazó eszközök esetében titkosítást írunk elő. A kriptográfiai programunkban matematikai technikákat alkalmazunk az információk és a kommunikáció biztosítására, biztosítva, hogy csak az arra jogosult felek férhessenek hozzá az adatokhoz. A HP információbiztonsági programjának kritikus eleme az adatok védelme a jogosulatlan hozzáféréstől és manipulációtól.

9. Fizikai és környezeti biztonság

   A HP létesítményeit különböző fizikai és elektronikus hozzáférés-ellenőrzésekkel, többek között biztonsági őrökkel, elektronikus hozzáférés-ellenőrzéssel és zártláncú térfigyelő berendezéssel (CCTV) biztosítják. A létesítmények fel vannak szerelve a szükséges infrastrukturális támogatással is, beleértve a hőmérséklet-szabályozást és a szünetmentes tápegységet és/vagy dízelgenerátorokat használó biztonsági tápegységeket a kritikus szolgáltatások támogatása érdekében. A HP teljes személyzete regisztrálva van, és köteles megfelelő azonosító jelvényt viselni.

10. Műveletkezelés

    A HP minimális védelemerősítő követelményeket állapított meg a technológiai infrastruktúrára, beleértve a munkaállomásokat, kiszolgálókat és hálózati berendezéseket. Ezek az eszközök előre megerősített védelemmel rendelkező operációsrendszer-képeket használnak, a követelmények operációs rendszerenként és a végrehajtott vezérlések szerint változnak. Emellett a HP olyan hálózati behatolásjelző/megelőző rendszereket (NIDS/NIPS) telepített, amelyeket a nap 24 órájában felügyelnek és kezelnek.

11. Kommunikációbiztonság

    A Kommunikációbiztonság biztosítja a vállalati hálózatokon belüli információk védelmét. Ez magában foglalja a hálózati biztonsági elemek (pl. tűzfalak) telepítését és kezelését, a hálózatok elkülönítését, valamint a webszűrést és az e-mail-kezelés ellenőrzését. Emellett magában foglalja a kommunikációs csatornák felügyeletét és kezelését a jogosulatlan hozzáférés vagy az adatok megsértésének felderítése és megelőzése érdekében.

12. Rendszerbiztonság

    A HP irányelve a rendszerek és szoftverek teljes életciklusa során biztonságos fejlesztési módszertant ír elő. A szoftverfejlesztési életciklus magában foglalja a bevezetést, a fejlesztést/beszerzést, a megvalósítást, az üzemeltetést és az ártalmatlanítást. Minden rendszerösszetevőt értékelünk az általános biztonságra gyakorolt hatásuk szempontjából. A HP ellenőrzéseket vezetett be az alkalmazásszolgáltatási tranzakciókhoz, beleértve a felhasználói hitelesítő adatok érvényesítését, a digitális aláírásokat, a titkosítást, a biztonságos kommunikációs protokollokat és a tranzakció részleteinek megfelelő hálózati biztonsági zónán belüli tárolását. Rendszeres belső biztonsági rések beolvasását is elvégezzük.

13. Külső felek és alvállalkozók

A HP folyamatokkal rendelkezik az olyan alvállalkozók kiválasztására, akik megfelelnek az átfogó szerződéses biztonsági követelményeknek. A HP vagy az ügyfelek adatait kezelő, illetve a HP hálózatához hozzáférő beszállítók esetében a HP Kiberbiztonsági kockázatértékelést végez a fizikai, technikai és adminisztratív biztosítékokat tartalmazó információbiztonsági program ellenőrzése érdekében. Ez az értékelés szükséges ahhoz, hogy a szállító hozzáférhessen a HP információkhoz.

14. Információbiztonsági incidens kezelése

A HP átfogó kiberincidens-kezelési folyamattal rendelkezik, amely meghatározza a célt, a hatásköröket, a szerepköröket, a felelősségi köröket, a vezetői elkötelezettséget, a szervezeti koordinációt, a végrehajtási eljárásokat és a megfelelőség ellenőrzését. Ezt a folyamatot felülvizsgáljuk és évente frissítjük. A Kiberincidensekre reagáló csoport, amely magában foglalja a HP kiberbiztonsági incidenskezelésre és válságkezelésre kiképzett munkatársait, rendszeres, veszélyhelyzetet szimuláló felülvizsgálatokat végez a folyamatról és az esetleges incidensekről vagy eseményekről.

15. Üzletmenet-folytonosság kezelése

A HP Globális működésfolytonossági programja az együttműködésen alapuló, szabványosított és dokumentált tervezési folyamatok révén biztosítja a végponttól végpontig tartó folytonosságot. A vállalat rendszeresen gyakorolja üzletmenet-folytonossági terveit a hatékonyság biztosítása érdekében, és legalább évente teszteli és frissíti az összes tervet. Ezenkívül az üzletmenet-folytonossági tervben részt vevő valamennyi munkatárs megfelelő képzésben részesül.

16. Megfelelőség

A megfelelőség határozza meg a HP megközelítését a hatékony információbiztonsági programmal kapcsolatos jogi, szerződéses és belső elvárások teljesítéséhez. A rendszeres információbiztonsági felülvizsgálatok biztosítják, hogy a protokollok beépüljenek az egyes üzleti csoportok működésébe. A felülvizsgálati folyamat a dokumentumokat a jelenlegi jogi kötelezettségeknek megfelelően is folyamatosan frissíti a szigorodó követelményeknek megfelelően.

17. Fizetésikártya-iparág

A Fizetésikártya-iparág (Payment Card Industry, PCI) keretrendszer irányítja a HP megközelítését a PCI-megfelelőség eléréséhez, felvázolva az üzleti felelősségköröket és a PCI DSS-hez igazított biztonsági ellenőrzéseket. A HP a hálózati biztonsági ellenőrzések, például tűzfalak telepítésével és karbantartásával biztosítja, hogy megfeleljen a PCI-megfelelőségi követelményeknek.

18. HP Termékbiztonság

    A HP Termékbiztonság olyan alapvető gyakorlatokat foglal magában, amelyek a HP-termékek biztonságát szolgálják, mint például a kódaláírás, a termékbiztonsági rések kezelése, a biztonsági tájékoztatók kiadása és a termékbiztonsági problémák jelentése. Ezek az intézkedések biztosítják, hogy a HP termékek biztonságosak és megbízhatóak legyenek a felhasználók számára. A HP-nál a termékbiztonság kiemelkedő fontosságú, mivel segít fenntartani az ügyfelek bizalmát, és védelmet nyújt a potenciális fenyegetésekkel szemben.

19. HP Szolgáltatásbiztonság

    A HP Szolgáltatásbiztonság a HP ügyfeleinek nyújtott szolgáltatások biztonságát szolgáló alapvető gyakorlatokat foglalja magában. Ez az irányelv a szolgáltatások biztonságának különböző területeivel foglalkozik, beleértve a HP infrastruktúra által üzemeltetett, a harmadik fél által üzemeltetett, a partner által üzemeltetett és az ügyfél által üzemeltetett környezeteket. Ezek az intézkedések biztosítják, hogy a HP szolgáltatásai biztonságosak és megbízhatóak legyenek a felhasználók számára. A megbízható biztonsági gyakorlatok bevezetésével a HP biztosítja termékeinek és szolgáltatásainak biztonságát és integritását, elősegítve a biztonságos és megbízható környezet kialakítását minden felhasználó számára.